945U-E wireless Ethernet modem user manual

Version 2.16

Powering Business Worldwide

Documentation Note

Eaton acquired Cooper Industries in November, 2012. “Cooper Bussmann” may appear in some screen images within this guide.

ATTENTION!

Incorrect termination of supply wires may cause internal damage and will void warranty. To ensure your 945U-E enjoys a long life, double check ALL your connections with the user manual before turning the power on.

CAUTION

To comply with FCC RF Exposure requirements in section 1.1310 of the FCC Rules, antennas used with this device must be installed to provide a separation distance of at least 20 cm from all persons to satisfy RF exposure compliance.

DO NOT

- Operate the transmitter when someone is within 20 cm of the antenna.
- Operate the transmitter unless all RF connectors are secure and any open connectors are properly terminated.
- Operate the equipment near electrical blasting caps or in an explosive atmosphere.

All equipment must be properly grounded for safe operation. All equipment should be serviced only by a qualified technician.

FCC Notice

This device complies with Part 15.247 of the FCC Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This device must be operated as supplied by ELPRO Technologies. Any changes or modifications made to the device without the written consent of ELPRO Technologies may void the user’s authority to operate the device.

End user products that have this device embedded must be installed by experienced radio and antenna personnel, or supplied with non-standard antenna connectors, and antennas available from vendors specified by ELPRO. Please contact ELPRO for end user antenna and connector recommendations.

In accordance with 47 CFR Part 15 Subpart C Section 15.203, only the following antenna/coax cable kits combinations can be used.

Manufacturer	Model Number	Coax Kit	Net
ELPRO	DG900-1	Includes 1m Cellfoil	-2 dB Loss
ELPRO	DG900-5	Includes 5m Cellfoil	-3 dB Loss
ELPRO	CFD890EL	Includes 5m Cellfoil	Unity Gain
ELPRO	SG-900EL	CC10/900	1.8 dB Gain
ELPRO	SG-900EL	CC20/900	-1.2 dB Loss
ELPRO	SG-900-6	CC10/900	4.8 dB Gain
ELPRO	SG-900-6	CC20/900	1.8 dB Gain
ELPRO	YU6/900	CC10/900	6.8 dB Gain
ELPRO	YU6/900	CC20/900	3.8 dB Gain

- Part 15—This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules (Code of Federal Regulations 47CFR Part 15). Operation is subject to the condition that this device does not cause harmful interference.

- Notice—Any changes or modifications not expressly approved by ELPRO could void the user's authority to operate this equipment.

This Device should only be connected to PCs that are covered by either FCC DoC or are FCC certified.

Safety

Exposure to RF energy is an important safety consideration. The FCC has adopted a safety standard for human exposure to radio frequency electromagnetic energy emitted by FCC regulated equipment as a result of its actions in Docket 93-62 and OET Bulletin 65 Edition 97-01.

UL Notice

1. The Wireless Ethernet module is to be installed by trained personnel / licensed electricians only and installation must be carried out in accordance with the instructions listed in the Installation Guide and applicable local regulatory codes.
2. The units are intended for Restricted Access Locations.
3. The Wireless Ethernet module is intended to be installed in a final enclosure, rated IP54, before use outdoors.
4. The Equipment shall be powered using an external Listed Power Supply with LPS outputs or a Class 2 Power Supply.
5. The Wireless Ethernet module must be properly grounded for surge protection before use.
6. If installed in a hazardous environment coaxial cable shall be installed in a metallic conduit.

GNU Free Documentation License

Copyright (C) 2009 Eaton.

Eaton is using a part of Free Software code under the GNU General Public License in operating the 945U-E product. This General Public License applies to most of the Free Software Foundation's code and to any other program whose authors commit by using it. The Free Software is copyrighted by Free Software Foundation, Inc., and the program is licensed "As is" without warranty of any kind. Users are free to contact Eaton at the email address Elpro-sales@eaton.com for instructions on how to obtain the source code used in the 945U-E.

A copy of the license is included in "Appendix E - GNU FREE DOC LICENSE."

Important Notice:

ELPRO products are designed to be used in industrial environments by experienced industrial engineering personnel with adequate knowledge of safety design considerations.

ELPRO radio products are used on unprotected license-free radio bands with radio noise and interference. The products are designed to operate in the presence of noise and interference. However, in an extreme cases radio noise and interference could cause product operation delays or operation failure. As with all industrial electronic products, ELPRO products can fail in a variety of modes due to misuse, age, or malfunction. We recommend that users and designers design systems using design techniques intended to prevent personal injury or damage during product operation, and provide failure tolerant systems to prevent personal injury or damage in the event of product failure. Designers must warn users of the equipment or systems if adequate protection against failure has not been included in the system design. Designers must include this Important Notice in operating procedures and system manuals.

These products should not be used in non-industrial applications or life-support systems without first consulting ELPRO.

1. A radio license is not required in some countries, provided the module is installed using the aerial and equipment configuration described in the *945U-E Installation Guide*. Check with your local distributor for further information on regulations.
2. Operation is authorized by the radio frequency regulatory authority in your country on a non-protection basis.

Although all care is taken in the design of these units, there is no responsibility taken for sources of external interference. Systems should be designed to be tolerant of these operational delays.

3. To avoid the risk of electrocution, the aerial, aerial cable, serial cables and all terminals of the 945U-E module should be electrically protected. To provide maximum surge and lightning protection, the module should be connected to a suitable ground/earth and the aerial, aerial cable, serial cables and the module should be installed as recommended in the Installation Guide.
4. To avoid accidents during maintenance or adjustment of remotely controlled equipment, all equipment should be first disconnected from the 945U-E module during these adjustments. Equipment should carry clear markings to indicate remote or automatic operation. For example, “This equipment is remotely controlled and may start without warning. Isolate at the switchboard before attempting adjustments.”
5. The 945U-E module is not suitable for use in explosive environments without additional protection.
6. The 945U-E operates using the same radio frequencies and communication protocols as commercially available off-the shelf equipment. If your system is not adequately secured, third parties may be able to gain access to your data or gain control of your equipment via the radio link. Before deploying a system make sure you have considered the security aspects of your installation carefully.

Release Notice

This is the November 2014 release of the *945U-E Ethernet Modem User Manual* version 2.16, which applies to version 2.16 modem firmware.

Follow Instructions

Read this entire manual and all other publications pertaining to the work to be performed before installing, operating, or servicing this equipment. Practice all plant and safety instructions and precautions. Failure to follow the instructions can cause personal injury and/or property damage.

Proper Use

Any unauthorized modifications to or use of this equipment outside its specified mechanical, electrical, or other operating limits may cause personal injury and/or property damage, including damage to the equipment. Any such unauthorized modifications: (1) constitute “misuse” and/or “negligence” within the meaning of the product warranty, thereby excluding warranty coverage for any resulting damage; and (2) invalidate product certifications or listings.

CONTENTS

Chapter 1 - INTRODUCTION 7
1.0 Network Topology 7
Access Point vs. Client 8
Bridge vs. Router 9
1.1 Getting Started Quickly 10

Chapter 2 - INSTALLATION 11
2.0 General. 11
2.1 Antenna Installation 11
Antenna Diversity 11
Bench Test and Demo System Setup 12
Plant and Factory Installations. 12
Line-of-sight Installations. 13
Antenna Gain and Loss 13
Installation Tips 13
Dipole and Collinear Antennas. 14
Directional Antennas 14
2.2 Power Supply. 15
2.3 Serial Connections. 16
RS232 Serial Port. 16
DB9 Connector Pinouts 16
RS485 Serial Port. 16
2.4 Discrete (Digital) Input/Output 17

Chapter 3 - OPERATION 19
3.0 Startup 19
Access Point Startup 19
Client Startup 19
Link Establishment. 19
How a Link Connection Is Lost 19
Roaming Clients. 19
LED Indication 20
3.1 Selecting a Channel. 20
802.11 (900 MHz) Channels. 20
Radio Throughput 21
Throughput and Repeaters 22
3.2 Configuring the Unit for the First Time 23
Default Configuration 23
Accessing Configuration for the First Time 23
3.3 Quick Start. 27
3.4 Network Configuration. 28
3.6 Security Menu 31
WEP (64 bit) and (128 bit) 32
Encryption Keys 1 to 4 32
Default WEP Key 32
WEP Open Authentication Mode 32
WEP Shares Authentication Mode 32
WPA / WPA2 32
WPA Enterprise - Authenticator (AP) Configuration 33
WPA Enterprise - Supplicant (Client) Configuration 34
3.7 Normal Operation 34
Bridge Operation (Transparent Network). 34
Router Operation (Routed Network) 35
3.8 Radio Configuration. 35
3.9 Advanced Radio Configuration 37
Fixed Noise Floor. 38
3.10 Serial Port Configuration 39
RS-232 PPP Server 39
Serial Gateway (Server/Client/Multicast) 40
Serial Gateway (Modbus–Modbus RTU to TCP) . 40
Modbus TCP to RTU Gateway 41
3.11 Serial Menu 42
RS-232 / RS485 Serial Port Configuration 42
RS232 PPP Server (Only RS232). 42
RS-232 / RS485 Serial Gateway Mode 42
RS-232 / RS485 Modbus TCP/RTU Converter . . 43
3.12 Multicast Pipe Manager. 44
3.13 Digital Input/Output 44
3.14 Modbus I/O Transfer 45
3.15 Roaming. 48
3.16 Repeaters (WDS) 50
3.17 Routing Rules. 57
3.18 Filtering 59
MAC Address Filter Configuration 60
IP Address Filter Configuration 61
ARP Filter Configuration 61
3.19 DHCP Client Configuration 62
3.20 DHCP Server Configuration. 62
3.21 DNS Server Configuration 62
3.22 VLAN 63
What is VLAN 63
Operation 63
VLAN Group. 65
Interface Membership 65
Examples 65
3.23 Module Information Configuration. 69
3.24 Configuration Examples 70
Setting a 945U-E to Factory Default Settings . . . 70
Extending a Wired Network. 70
Connecting Two Networks Together. 71
Extending Network Range with a Repeater Hop. 73

Chapter 4 - DIAGNOSTICS 74
4.0 Diagnostics Chart 74
4.1 Connectivity. 74
Connectivity Parameters 75
Site Survey. 75

4.2 Channel Survey (Utilization) 75
Channel Utilization on a Live System 76
Channel Utilization for Channel Selection or RF Path Testing 76
Diagnosing Low Throughput 76
Solutions for High Channel Utilization 76
4.3 Custom Survey 78
4.4 Throughput Test 79
Internal Throughput Test 80
4.5 Statistics 82
Wireless Statistics 82
Network Traffic Analysis 83
4.6 System Tools 83
4.7 Testing Radio Paths. 84
Connection and Signal Strength 84
Throughput Test. 84
Internal Radio Tests 84
RSSI Test. 85
Throughput Test 85
4.8 Remote Configuration 86
4.9 Internal Diagnostic Modbus Registers 87
Connection Information 87
Statistic Registers 88
4.10 Utilities 88
ping 88
ipconfig. 90
arp 90
route 90

Chapter 5 - SPECIFICATIONS 92

Appendix A - FIRMWARE UPGRADES 94
Web-based Upgrade 94

Appendix B - GLOSSARY 95

Appendix C - POWER CONVERSION 100
Power Conversion 100

Appendix D - IPERF THROUGHPUT TEST - EXT. 101
Materials. 101
Installation 101
Iperf Application. 101
JPerf Application 103

Appendix E - GNU FREE DOC LICENSE 104

CHAPTER 1 - INTRODUCTION

The 945U-E Wireless Ethernet Modem and Device Server is an industrial 802.11-compliant module that provides wireless connections between Ethernet devices and/or Ethernet wired networks (LANs) and complies with relevant IEEE 802.11 standards.

945U-E 802.11	630mW max power
945U-E-H	802.11 1000mW max power

The 945U-E is a Direct Sequence Spread Spectrum (DSSS) wireless transceiver that utilizes the unlicensed 900-MHz frequency band for communications. There are various channels and bandwidths available depending on the country and their radio regulations. If operating in the North America you can choose from the following 9 x 1.25 MHz, 9 x 2.5 MHz, 4 x 5 MHz, 4 x 10 MHz or 2 x 20 MHz channels. If operating in Australia you can choose from 4 x 1.25 MHz, 4 x 2.5 MHz, 3 x 5 MHz or 1 10 MHz channels, etc. For a more information see “3.1 Selecting a Channel.”

The 945U-E unit also provides two serial connections as well as the Ethernet connections. It is possible to use all three data connections concurrently, allowing the 945U-E to act as a Device Server. Wireless connections can be made between serial devices and Ethernet devices. The 945U-E provides connection functionality between serial “Modbus RTU” devices and Ethernet “Modbus TCP” devices. Appropriate driver applications will be required in the host devices to handle other protocols.

The modem is VLAN compliant and capable of passing VLAN tagged frames by default. VLAN bridging and Routing Modes are also available which will facilitate a number of different VLAN topologies.

The 945U-E has a standard RJ45 Ethernet connection which will operate at up to 100 Mbit/sec. The module will transmit the Ethernet messages on the wireless band at rates between 1 and 54 Mbit/sec & 6 and 54 Mbit/sec depending on model, band, encryption methods, and radio paths.

1.0 Network Topology

The 945U-E is an Ethernet device, and must be configured as part of an Ethernet network. Each 945U-E must be configured as an:

- Access Point or Sta, Station, Client

Also needs to be configured as a:

- Bridge or Router

You can also connect to the 945U-E via an RS232 or RS485 serial port using serial server or point-to-point (PPP) protocol. PPP allows the 945U-E to connect serial communications into the Ethernet network.

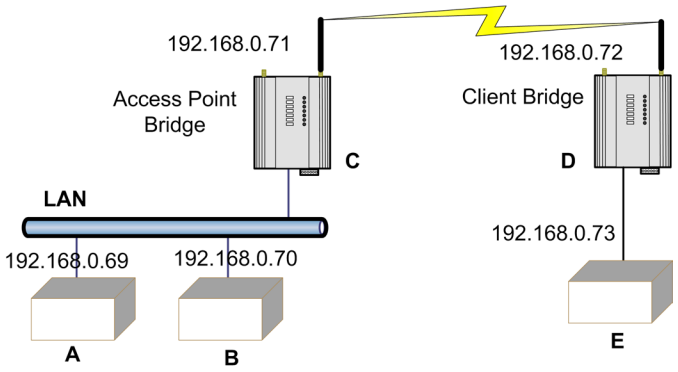


Figure 1 Network Topology

Access Point vs. Client

The Access Point unit acts as the wireless master unit. The Access Point accepts and authorizes links initiated by client units, and controls the wireless communications.

Clients (Stations) are slave units and when connected to the Access Point become transparent Ethernet links.

Figure 2 shows a connection between two Ethernet devices using 945U-E Ethernet modems. In this example one 945U-E is configured as an Access Point and the other as a Client. The Access Point can be connected.

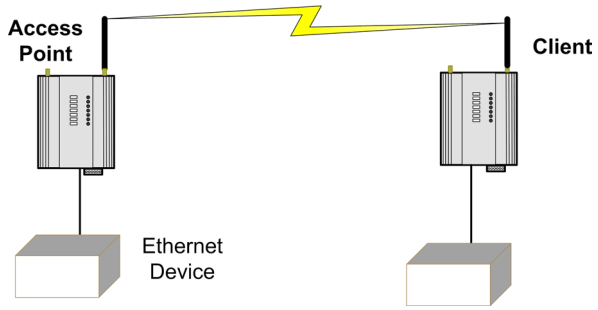


Figure 2 Access Point and Client (Example 1)

Figure 3 shows an existing LAN being extended using 945U-Es. In this example, the Access Point is configured at the LAN end, although the wireless link will still work if the Client is at the LAN end.

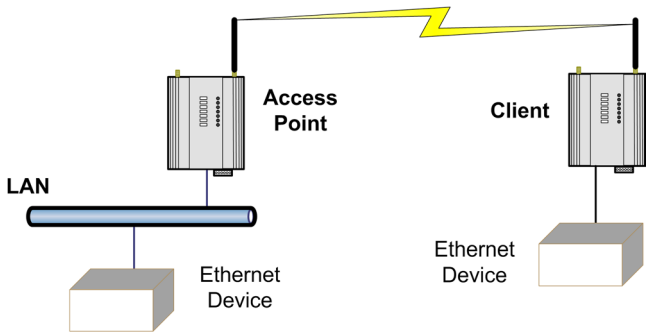


Figure 3 Access Point and Client (Example 2)

An Access Point can connect to multiple Clients. In this case, the Access Point should be the central unit.

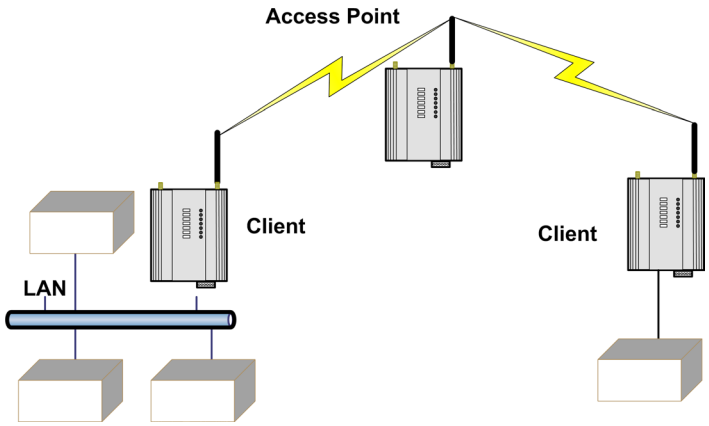


Figure 4 Repeater

An Access Point could be used as a repeater unit to connect two 945U-E Clients that do not have direct reliable radio paths. There is no special repeater module—any 945U-E can be a repeater and at the same time can be connected to an Ethernet devices or on a LAN.

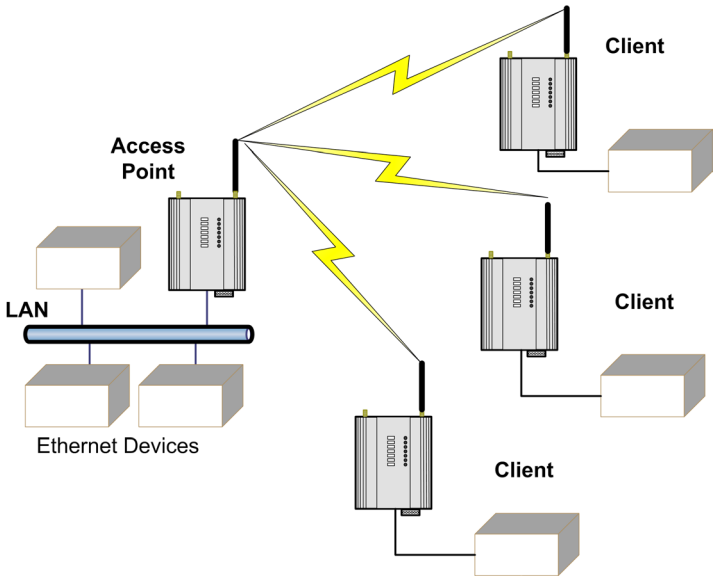


Figure 5 Multiple Clients

Multiple Access Points can be set up in a mesh network to provide multiple repeaters.

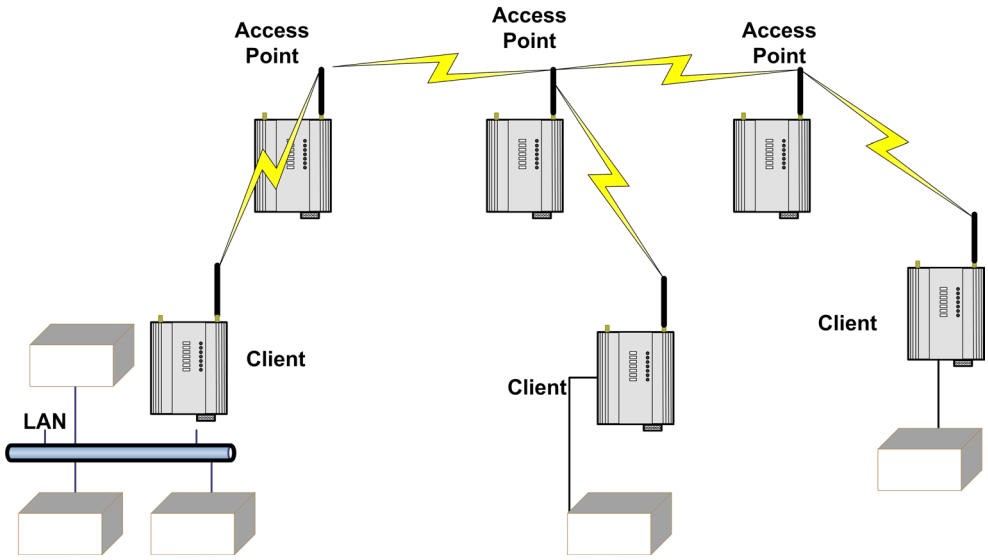


Figure 6 Multiple Access Points

Bridge vs. Router

Each 945U-E is configured with one IP address for the Ethernet side and another for the wireless side. A Bridge connects devices within the same Ethernet network, for example, extending an existing Ethernet LAN. For a Bridge, the IP address for the wireless side is the same as the Ethernet side.

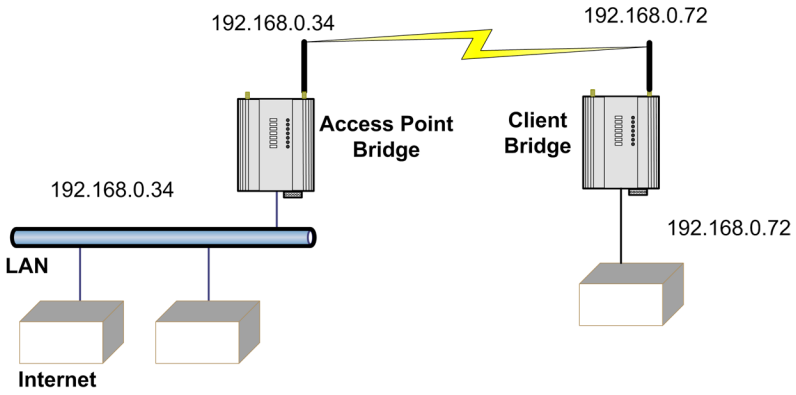


Figure 7 Bridge

A Router connects devices on different LANs. The IP addresses for the Ethernet and wireless sides are different. In the example in Figure 8, the wireless link is part of LAN A with the Client unit acting as a Router between LAN A and LAN B.

Alternatively, the Access Point could be configured as a Router. The wireless link is then part of LAN B. If more than two routers are required within the same radio network, then routing rules may need to be configured (see “3.17 Routing Rules” for details). There is no limit to the number of Bridges in the same network, although there is a limit of 128 Client units linked to any single Access Point.

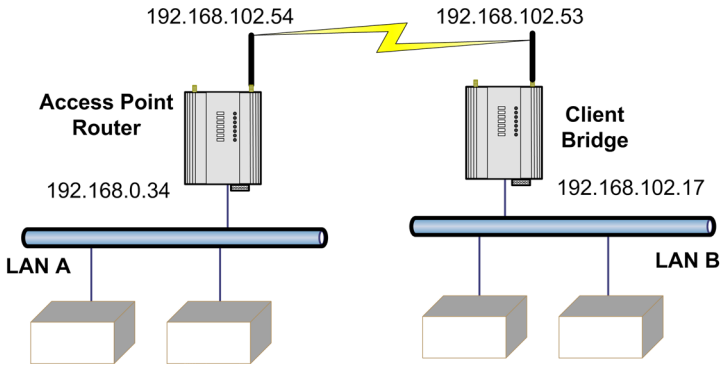


Figure 8 Router

1.1 Getting Started Quickly

Most applications for the 945U-E require little configuration. The 945U-E has many sophisticated features, but if you do not require these features you can use this section to configure the units quickly.

To get started quickly:

1. Read “Chapter 2 - INSTALLATION.” The 945U-E requires an antenna and a power supply.
2. Power the 945U-E and make an Ethernet connection to your PC.

   For detailed steps, see “3.2 Configuring the Unit for the First Time.”
3. Set the 945U-E address settings as described in “3.2 Configuring the Unit for the First Time.”
4. Save the configuration.

   The 945U-E is now ready to use.

Before installing the 945U-E, bench test the system. It is much easier to locate problems when the equipment is altogether. There are additional configuration settings, that may improve the operation of the system. For more information, see “3.0 Startup.”

CHAPTER 2 - INSTALLATION

2.0 General

The 945U-E modules are housed in a rugged aluminum case suitable for DIN-rail mounting. Terminals will accept wires up to 2.5 mm2 (12 gauge) in size. All connections to the module must be SELV (Safety Extra Low Voltage). Normal 110-250V mains supply must not be connected to any terminal of the 945U-E module. Refer to “2.2 Power Supply.”

Before installing a new system, it is preferable to bench test the complete system. Configuration problems are easier to recognize when the system units are adjacent. Following installation, the most common problem is poor communications caused by incorrectly installed antennas, radio interference on the same channel, or the radio path being inadequate. If the radio path is a problem (for example, the path is too long or obstructed), a higher performance antenna or a higher mounting point for the antenna may rectify the problem. Alternatively, use an intermediate 945U-E module as a repeater.

The *945U-E Installation Guide* provides an installation drawing appropriate to most applications. Further information is detailed below. Each 945U-E module should be effectively earthed via the “GND” terminal on the back of the module. This is to ensure that the surge protection circuits inside are effective.

2.1 Antenna Installation

The 945U-E module will operate reliably over large distances. However, the achievable distances will vary with the application, radio model, type and location of antennas, the degree of radio interference, and obstructions (such as buildings or trees) to the radio path.

The maximum range achievable depends on the radio model, the regulated RF power permitted in your country, and whether you use separate transmit and receive antennas. A 945U-E (900 MHz) with a single antenna, 6.2 miles can be achieved in USA, Canada (4W ERP) and 10 km in Australia, New Zealand (1W ERP).

To achieve the maximum transmission distance, the antennas should be raised above intermediate obstructions so the radio path is true line-of-sight. The modules will operate reliably with some obstruction of the radio path, although the reliable distance will be reduced. Obstructions that are close to either antenna will have more of a blocking affect than obstructions in the middle of the radio path.

The 945U-E modules provide a diagnostic feature that displays the radio signal strength of transmissions. Refer to “Chapter 4 - DIAGNOSTICS.”

Line-of-sight paths are only necessary to obtain the maximum range. Obstructions will reduce the range, however may not prevent a reliable path. A larger amount of obstruction can be tolerated for shorter distances. For short distances, it is possible to mount the antennas inside buildings. An obstructed path requires testing to determine if the path will be reliable. Refer to “4.7 Testing Radio Paths.”

Where it is not possible to achieve reliable communications between two 945U-E modules, then a third 945U-E module may be used to receive the message and re-transmit it. This module is referred to as a repeater. This module may also have a host device connected to it.

The 945U-E unit has two antenna connections at the top of the module, allowing for two antennas to be fitted to the module if need be. By default the right connector labeled TX/RX is the main connection used to transmitter and receiver. The left connector, labeled “RX,” is not connected unless configured as described in “3.9 Advanced Radio Configuration.” Each antenna port can be configured for TX only, RX only or Diversity (TX and RX). Selection can be made by choosing one of the options from TX Antenna/RX Antenna on the Advanced Radio Configuration page.

NOTE When only one antenna is used, it must be connected to the TX/RX connector.

Antenna Diversity

There are two main reasons for using Antenna diversity. The first is to improve the reliability of a radio link that may be affected by multipath signals. Often if radio signals are transmitted in built-up area the signal can get reflected off different surfaces and when these signals are received they can cancel each other out due to slightly different

time delays. Using more than one antenna the radio is able to choose the best signal thus providing a more robust radio link.

The second reason to use antennas diversity is to increase the received radio signal into the receiver. All countries have radio licensing regulations that can often limit on the amount of transmitted power and radiated power from the antenna. In the US this is 630 mW or 1000 mW for the 945U-E-H of transmit power and 4 watts EIRP (Effective Isotropic Radiated Power) from the antenna. If a high gain antenna is used to try and improve the receive signal it will also increase the transmit level and push it over the EIRP regulation limit.

Using Antenna diversity allows two antennas to be used, one for receive and the other for transmit/receive. The TX/RX antenna has the normal restriction on gain to keep it below the regulation limit. However, the receive antenna has no regulatory limits as it does not radiate power so a higher gain antenna can be used to receive weaker signals. See “3.9 Advanced Radio Configuration” for details on configuring Antenna diversity.

In North America, the maximum allowable radiated power (EIRP) for a 945U-E is 4 Watts, which is 8 dB higher that the modules transmit power of 630 mW or 6 dB higher that the transmit power of the 945U-E-H. Therefore we are able to increase the antenna gain as long as overall system gain (antenna Gain – coax loss) does not go above 8 dB for the 945U-E or 6 dB for the 945U-E-H.

Example

- Using the 945U-E with 10 m (33 ft) of Cellfoil coax cable (approximately 3 dB of loss) and an 8 dBi collinear antenna would equate to approximately 5 dB of gain, which is below the regulated 8 dB limit.
- Using the 945U-E-H with 20 m (66 ft) of Cellfoil coax cable (approximately 6 dB of loss) and a 10 dBi Yagi antenna would equate to approximately 4 dB of gain, which is below the regulated 6 dB limit.

Bench Test and Demo System Setup

Care must be taken with placement of antenna in relation to the radios and the other antennas. Strong radio signals can saturate the receiver, hindering the overall radio communications.

When setting up a bench test, demo, or a short range system, the following considerations should be taken into account for optimum radio performance and reduced signal saturation.

- If using Demo Whip antennas (DG-900 and WH-900), it is recommended that only the Access Point be fitted with an antenna.
- If using Demo Whip antennas on each end, a 20 dB coax attenuator must be connected in-line with the coax cable.
- If using Demo Whip antennas, modules and antennas must be kept a suitable distance from each other. Check the receive signal strength on the Connectivity page of the module and ensure the level is not greater than -45 dB.

Demo Whip antennas should not be used in the final installation as the maximum performance of the modem cannot be guaranteed. If using a DG-900 antenna, it is better to keep the antennas at least 3 ft (1 m) away from the module so as to limit RF saturation.

Plant and Factory Installations

Another application where antenna diversity may be needed is in industrial plants and factories installations which can suffer from multipath fading effects where multiple reflected radio signals adversely affect the signal strength. In a static installation where the radio path is not changing, moving an antenna to the position of maximum signal solves this problem. However, where the radio path changes because the 945U-E is mounted on moving equipment or if there is moving equipment in the area, the solution is to use two antennas. Because the two connectors are separated, the RF signal at each connector will be different in the presence of multi-path fading. The 945U-E unit will automatically select the higher RF signal provided RX diversity has been enabled on the radio Configuration page.

Line-of-sight Installations

In longer line-of-sight installations, the range may be increased by using a high gain antenna on the TX/RX connector. However, the gain should not cause the effective radiated power (ERP) to exceed the permitted value. A second higher gain antenna can be connected to the RX connector without affecting ERP. This will increase the operating range provided any interference in the direction of the link is low.

Antenna Gain and Loss

Antennas can be either connected directly to the module connectors or connected via 50-ohm coaxial cable (for example, RG58 Cellfoil or RG213) terminated with a male SMA coaxial connector. The higher the antenna is mounted, the greater the transmission range will be. However, cable losses also increase as the length of the coaxial cable increases.

The net gain of an antenna-cable configuration is the gain of the antenna (in dBi) less the loss in the coaxial cable (in dB). The 945U-E maximum net gain for US and Canada is 10dB (4W ERP) and 0dB for Australia and NZ (1 W ERP). There is no gain restriction for antennas connected to the RX connector unless “TX Diversity” is enabled on the Radio page.

The gains and losses of typical antennas are as follows.

Antenna	945U-E Gain (dBi)
Dipole	0 dB
Collinear	5 or 8 dBi
Directional	10–15 dBi
Cable Loss	dB per 30 m/100 ft
RG58 Cellfoil	-9 dB
RG213	-7.4 dB
LDF4-50	-2 dB

The net gain of the antenna/cable configuration is determined by adding the antenna gain and the cable loss. For example, an 8 dBi antenna (5.8 dBd) with 10 meters of Cellfoil (3 dBd) has a net gain of 2.8 dB (5.8 dB–3 dB).

Installation Tips

Connections between the antenna and coaxial cable should be carefully taped to prevent ingress of moisture. Moisture ingress in the coaxial cable is a common cause for problems with radio systems, as it greatly increases the radio losses. We recommend that the connection be taped, firstly with a layer of PVC Tape, then with a vulcanizing tape such as 3M™ 23 tape and finally with another layer of PVC UV-stabilized insulating tape. The first layer of tape allows the joint to be easily inspected when trouble shooting as the vulcanizing seal can be easily removed.

Where antennas are mounted on elevated masts, the masts should be effectively earthed to avoid lightning surges. For high lightning risk areas, approved ELPRO surge suppression devices such as the CSD-SMA-2500 or CSD-N-6000 should be fitted between the module and the antenna. If using non ELPRO surge suppression devices, the devices must have a TURN ON voltage of less than 90 V. If the antenna is not already shielded from lightning strike by an adjacent earthed structure, a lightning rod may be installed above the antenna to provide shielding.

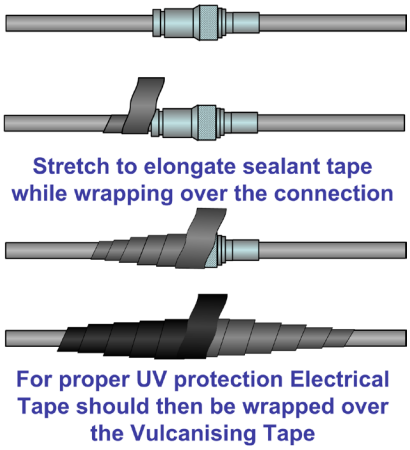


Figure 9 Vulcanizing Tape

Dipole and Collinear Antennas

A dipole or collinear antenna transmits the same amount of radio power in all directions—as such they are easy to install and use. The dipole antenna with integral 15 ft (5 m) cable does not require any additional coaxial cable. However, a cable must be used with the collinear antennas. To obtain maximum range, collinear and dipole antennas should be mounted vertically, preferably 1 wavelength away from a wall or mast (see Figure 10 for distances), and at least 3 ft (1 m) from the radio module.

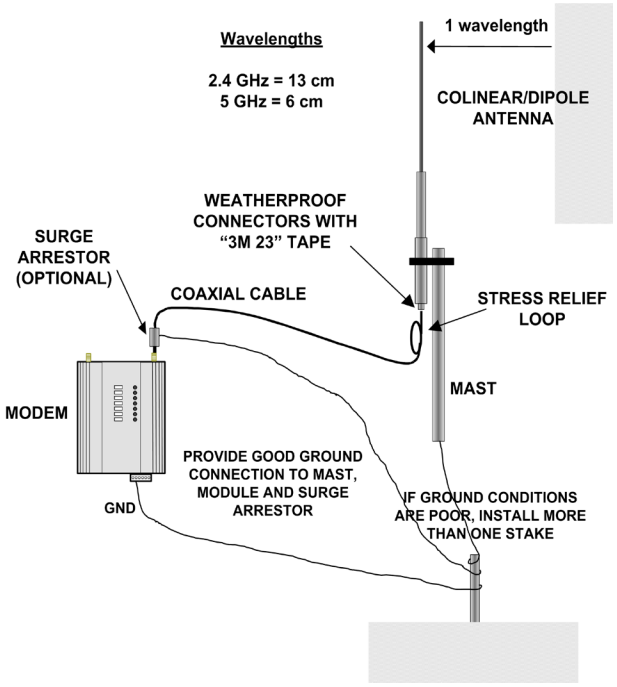


Figure 10 Collinear/Dipole Antenna

Directional Antennas

Directional antennas can be any of the following:

- Yagi antenna with a main beam and orthogonal elements.
- Directional radome, which is cylindrical in shape.
- Parabolic antenna.

A directional antenna provides high gain in the forward direction, but lower gain in other directions. This type of antenna may be used to compensate for coaxial cable loss for installations with marginal radio path.

Yagi antennas should be installed with the main beam horizontal, pointing in the forward direction. If the Yagi is transmitting to a vertically mounted omni-directional antenna, the Yagi elements should be vertical. If the Yagi is transmitting to another Yagi, the elements at each end of the wireless link need to in the same plane (horizontal or vertical).

Directional radomes should be installed with the central beam horizontal and must be pointed exactly in the direction of transmission to benefit from the gain of the antenna. Parabolic antennas should be mounted as per the manufacturer's instructions, with the parabolic grid at the back and the radiating element pointing in the direction of the transmission.

Ensure that the antenna mounting bracket is well connected to ground/earth.

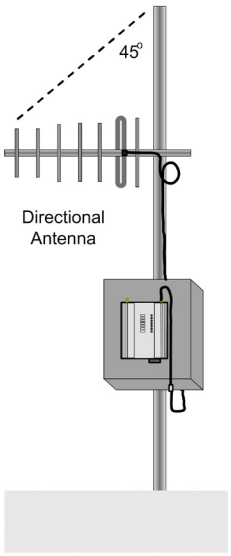


Figure 11 Dipole Antenna

2.2 Power Supply

The 945U-E module can be powered from a 9–30 Vdc power supply. The power supply should be rated at 1 Amp minimum. The positive side of the supply must not be connected to earth. The supply negative is connected to the unit case internally. The DC supply may be a floating supply or negatively grounded.

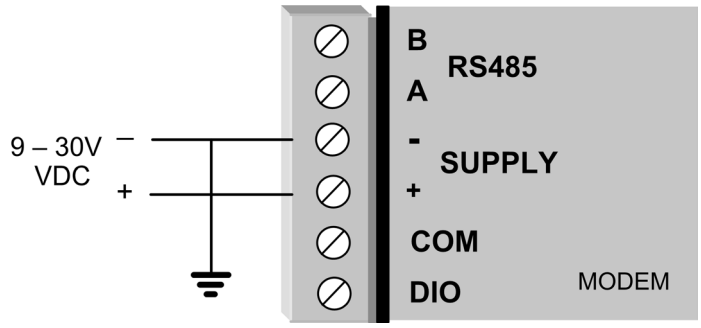


Figure 12 Power Supply

The power requirements of the 945U-E unit are shown in the following table.

	12Vdc	24Vdc
Quiescent	300 mA	160 mA
TX @100 mW	370 mA	190 mA
TX @ 400 mW	410 mA	210 mA

A ground terminal is provided on the back of the module. This terminal should be connected to the main ground point of the installation in order to provide efficient surge protection for the module (refer to the Installation diagram).

2.3 Serial Connections

RS232 Serial Port

The serial port is a 9-pin DB9 female and provides for connection to a host device as well as a PC terminal for configuration, field testing, and factory testing. Communication is via standard RS232 signals. The 945U-E is configured as DCE equipment with the pinouts described below.

Hardware handshaking using the CTS/RTS lines is provided. The CTS/RTS lines may be used to reflect the status of the local unit's input buffer. The 945U-E does not support XON/XOFF. Example cable drawings for connection to a DTE host (a PC) or another DCE hosts (or modem) are detailed in Figure 13.

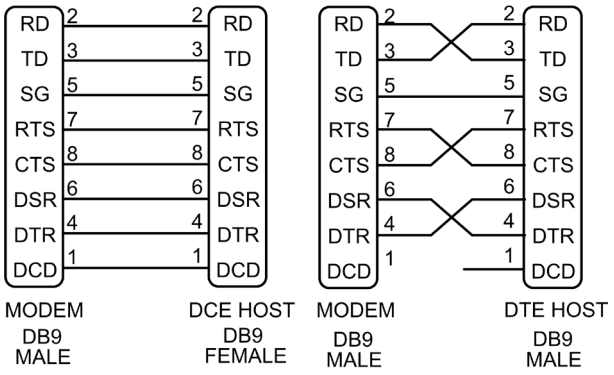


Figure 13 Serial Cable

DB9 Connector Pinouts

DB9 Connector Pinouts			
Pin	**Name**	**Direction**	**Function**
1	DCD	Out	Data Carrier Detect
2	RD	Out	Transmit Data – Serial Data Output (from DCE to DTE)
3	TD	In	Receive Data – Serial Data Input (from DTE to DCE)
4	DTR	In	Data Terminal Ready
5	SG		Signal Ground
6	DSR	Out	Data Set Ready - always high when unit is powered on
7	RTS	In	Request to Send
8	CTS	Out	Clear to Send
9	RI		Ring Indicator

RS485 Serial Port

The RS485 port provides for communication between the 945U-E unit and its host device using a multi-drop cable. Up to 32 devices may be connected in each multi-drop network.

Because the RS485 communication medium is shared, only one of the units on the RS485 cable may send data at a time. Therefore, communication protocols based on the RS-485 standard require some type of arbitration.

RS485 is a balanced differential standard, but it is recommended that shielded twisted pair cable be used to interconnect modules to reduce potential RFI. It is important to maintain the polarity of the two RS485 wires. An RS485 network should be wired as indicated in the diagram below and terminated at each end of the network with a 120-ohm resistor. On-board 120-ohm resistors are provided and may be engaged by operating the single DIP switch in the end plate next to the RS485 terminals. The DIP switch should be in the “1” (on) position to connect the resistor. If the module is not at one end of the RS485 cable, the switch should be off.

NOTE Shorter runs of 485 cables may not require the termination resistors to be enabled.

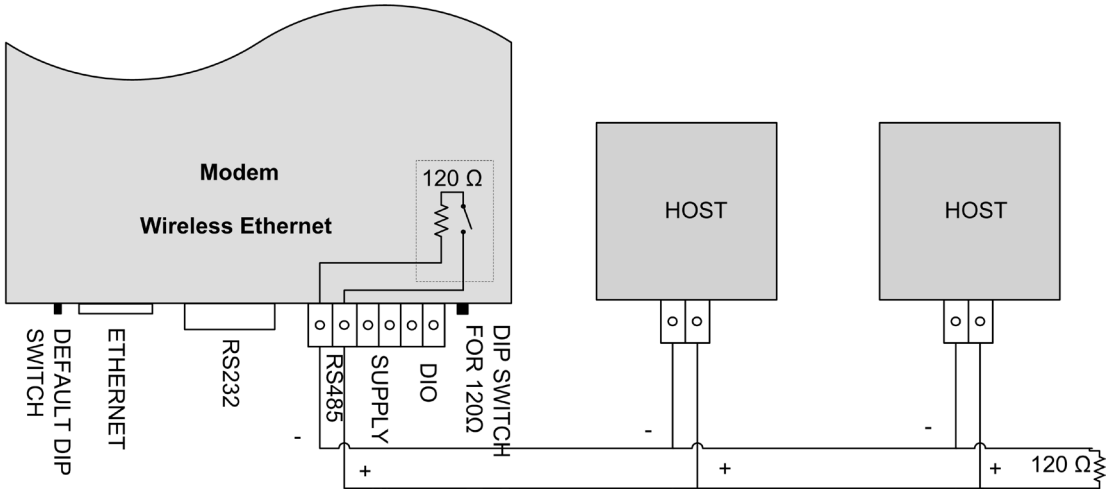


Figure 14 Multidrop Serial

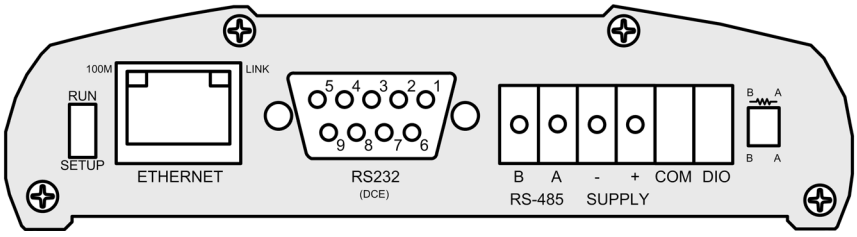


Figure 15 End Plate

2.4 Discrete (Digital) Input/Output

The 945U-E has one on-board discrete/digital I/O channel. This channel can act as either a discrete input or discrete output. It can be monitored, set remotely, or alternatively used to output a communications alarm status.

If used as an input, the I/O channel is suitable for voltage-free contacts (such as mechanical switches) or NPN transistor devices (such as electronic proximity switches). PNP transistor devices are not suitable. Contact wetting current of approximately 5 mA is provided to maintain reliable operation of driving relays.

The digital input is connected between the DIO terminal and common COM. The I/O circuit includes a LED indicator which is green when the digital input is active, that is, when the input circuit is closed. Provided the resistance of the switching device is less than 200 ohms, the device will be able to activate the digital input.

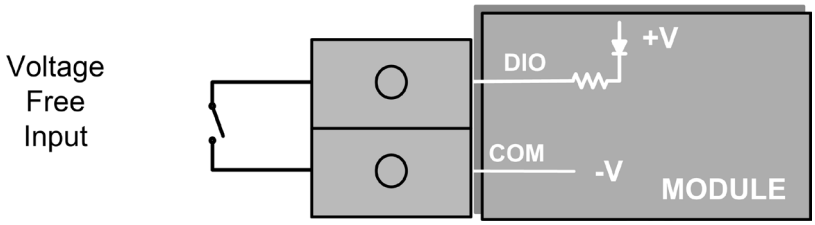


Figure 16 DIO Input

The I/O channel may also be used as a discrete output. The digital outputs are transistor switched DC signals, FET output to common rated at 30 Vdc 500 mA.

NOTE The output circuit is connected to the "DIO" terminal. The digital output circuit includes a LED indicator which is red when the digital output is active.

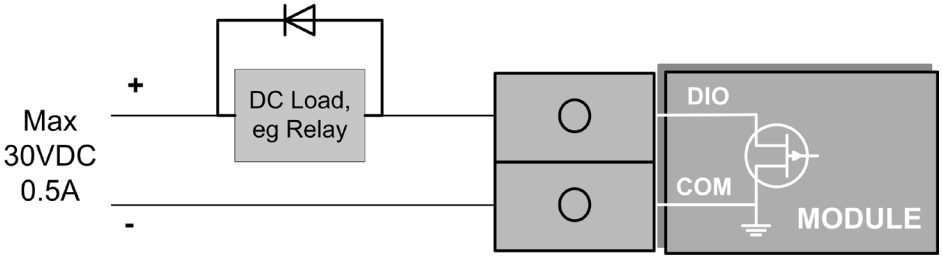


Figure 17 DIO Output

CHAPTER 3 - OPERATION

3.0 Startup

Access Point Startup

When an access point (AP) unit starts up, it will immediately begin transmitting periodic messages (beacons) on the configured channel. Beacons include information that a client may examine in order to identify if the access point is suitable for link establishment. Clients will only attempt to establish a link with an access point whose beacon indicates a matching SSID. Access points do not initiate link establishment.

Client Startup

When a client powers up, it scans for beacons from access points. While a link is not established, the client cyclically scans all available channels for a suitable access point. The client will attempt to establish a link with an access point only if it has matching SSID, encryption method, and other compatible capabilities as indicated by the beacon. If more than one suitable access point is discovered, the client will attempt to establish a link with the access point that has the strongest radio signal.

Link Establishment

Once a client identifies a suitable access point for link establishment, it attempts to establish a link using a two-step process—authentication, and association. During authentication, the client and access point check if their configurations permit them to establish a link. Once the client has been authenticated, it will request an association to establish a link.

Status of the wireless link is indicated via the TX/LINK LED. For an access point, the TX/LINK LED will be off as long as no links have been established. Once one or more links have been established, the TX/LINK LED is on green. For a client, the Link LED will reflect the connection status to an access point. Link status is also displayed on the Connectivity page of the Web interface.

After the link is established, data may be transferred in both directions. The access point will act as a master unit and will control the flow of data to the clients linked to it. Clients can only transmit data to the access point to which they are connected. When a client transfers data to another client, it first transmits the data to the access point, which then forwards the data to the destined client. A maximum of 127 clients may be linked to an access point.

NOTE The presence of a link does not mean that the connected unit is authorized to communicate over radio. If the encryption keys are incorrect between units in the same system, or a dissimilar encryption scheme is configured, the Link LED turns on, but data cannot be passed over the wireless network.

How a Link Connection Is Lost

The access point refreshes the link status with a client every time a message is received from that client. If nothing is received from a client for a period of 120 seconds, the access point sends a “link-check” message. If there is no response to the link check a de-authenticate message is sent and the link is dropped.

A client monitors beacon messages from an access point to determine whether the link is still present. If the client can no longer receive beacons from the access point it assumes the access point is out of range and the link is dropped. Whenever a Client is not connected to an access point, it will cyclically scan all available channels for a suitable access point.

Roaming Clients

Clients can roam within a system, but if the link to the access point fails or the radio signal level becomes too weak it will scan for beacons and connect to an access point (provided the SSID and any encryption methods, keys are compatible). If there are multiple access points, it selects the connection with the best signal level. This functionality permits a client to have mobility while maintaining a link with the most suitable access point.

LED Indication

The following table details the status of the indicating LEDs on the front panel under normal operating conditions.

LED Indicator	Condition	Meaning
OK	Green	Normal operation.
OK	Flashing Red/Green	Module boot sequence.
Radio RX	Green flash	Radio receiving data (good signal strength).
Radio RX	Red flash	Radio receiving data (low signal strength).
TX/LINK	Green	Radio connection established.
TX/LINK	Red flash	Radio transmitting.
RS-232	Green flash	Data dent from RS-232 serial port.
RS-232	Red flash	Data received yo RS-232 serial port.
LAN	On	Link established on Ethernet port.
LAN	Flash	Activity on Ethernet port.
RS-485	Green flash	Data sent from RS-485 serial port.
RS-485	Red flash	Data received To RS-485 serial port.
DIO	Green	Digital input is grounded.
DIO	Red	Digital output is active.
DIO	Off	Digital output off and input is open circuit.

The Ethernet RJ45 port incorporates two indication LEDs. The Link LED comes on when there is a connection on the Ethernet port, and will blink off briefly when activity is detected on the Ethernet port. The 100-MB LED indicates that the connection is at 100 MBit/sec. The 100-MB LED will be off for 10 MB/sec connection. Other conditions indicating a fault are described in “Chapter 4 - DIAGNOSTICS.”

3.1 Selecting a Channel

802.11 (900 MHz) Channels

The 945U-E conforms to the IEEE 802.11 Wireless LAN specification and supports various channels depending on regulations within the country of use.

If operating in the US, Canada, the frequency range is 902–928 MHz and the available channels are as follows:

- 9 x non overlapping 1.25-MHz channels
- 9 x partially overlapping 2.5-MHz channels
- 4 x non overlapping 5-MHz channels
- 4 x overlapping 10-MHz channels
- 2 x overlapping 20-MHz channels

If operating in Australia, the frequency range is 915–928 MHz and the available channels are as follows:

- 4 x non overlapping 1.25-MHz channels
- 4 x partially overlapping 2.5-MHz channels
- 3 x overlapping 5-MHz channels
- 1 x 10-MHz channel

If operating in Hong Kong, the frequency range is 922–925 MHz and the available channels are as follows:

- 2 x non overlapping 1.25-MHz channels
- 1 x 2.5-MHz channel

Regions will only show the available channels for that location. Figure 18 shows the frequency ranges and channels.

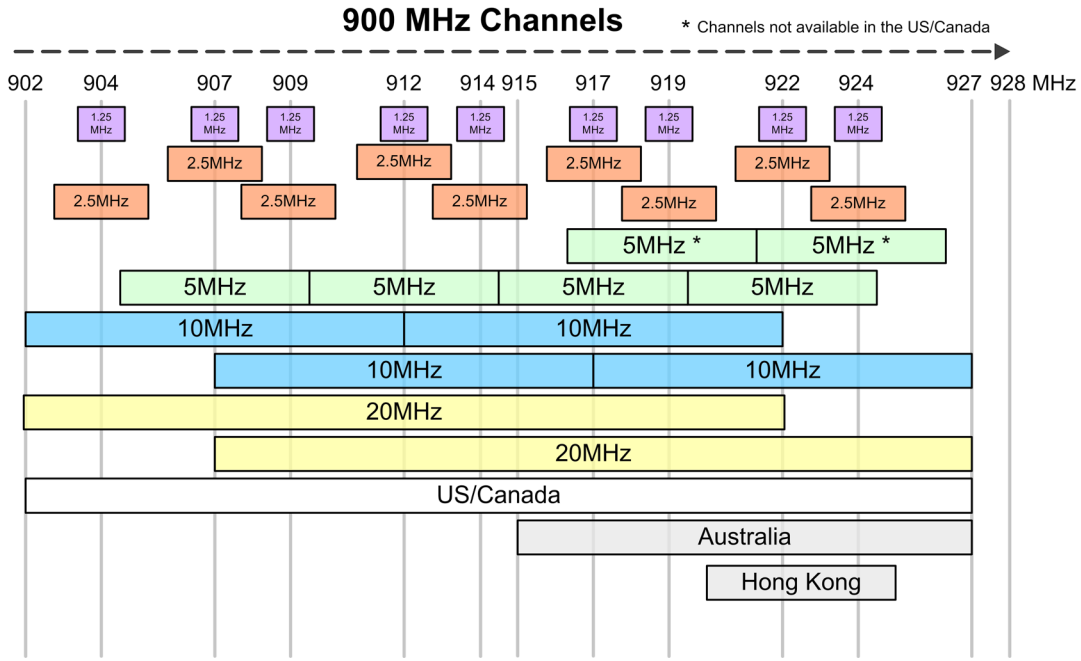


Figure 18 900MHz Channels

Each country or region has a different frequency regulation with multiple band widths and numerous channels available. The main reason for having different channels and bandwidths is to allow multiple radios to operate in close proximity with minimal interference. As you can see from the Channels Diagram (above) and the Data Throughput Table (in the following section), the greater the band width, the greater the overall data throughput.

If selecting the high band width, for example 20 MHz, you will be limited to one channel, which may be more susceptible to outside interference because it spans the available 900-MHz frequency range. In some regions this high band width option may not even be available. If selecting the lower bands, for example 1.25 MHz, you have more channels available and each channel is non-overlapping (adjacent channels do not cross over). However, the data throughput will be considerably lower. If you require high data throughput, the higher band width will need to be selected and care will also need to be taken with antenna placement.

Selecting a 20-MHz channel will give the maximum TCP/IP throughput of around 22 Mbps, but if the band width is reduced (for example, 10 MHz or 5 MHz) the maximum data throughput will also be reduced. For an indication of the data throughput levels used with different channel bandwidths see the 945U-E Radio Data Throughput table in the next section.

Radio Throughput

Below is a table showing the maximum TCP/IP throughput based on channel selection and receiver signal level. There are five channel bandwidths (20, 10, 5, 2.5, and 1.25 MHz). These throughput estimations are based on perfect radio conditions that assume little to no outside radio interference present while data is being passed, and they are calculated using real-life conditions and communication constraints. Higher data rates are achievable by using an external Iperf arrangement. For details, see “4.4 Throughput Test.”

945U-E Radio Data Throughput					
900MHz	Data Rate in Mbps				
Signal Strength	20MHz	10MHz	5MHz	2.5MHz	1.25MHz
-72 dBm	22.0	11.0	5.5	2.8	1.4
-75 dBm	20.0	10.0	5.0	2.5	1.3
-81 dBm	17.0	8.5	4.3	2.1	1.1
-84 dBm	11.0	5.5	2.8	1.4	0.7
-88 dBm	9.0	4.5	2.3	1.1	0.6
-91 dBm	6.0	3.0	1.5	0.75	0.38
-90 dBm	5.5	2.8	1.4	0.69	0.34
-91 dBm	4.5	2.3	1.1	0.56	0.28
-92 dBm	3.0	1.5	0.75	0.38	0.19
-91 dBm	2.0	1.0	0.5	0.25	0.13
-93 dBm	1.0	0.50	0.25	0.13	0.06
-95 dBm	0.5	0.25	0.13	0.06	0.03

Throughput and Repeaters

It should also be noted that if using repeaters to extend the range there will be a reduction in throughput for each repeater hop. The following tables show the drop in throughput for each hop and for each of the channel widths.

Data Throughput Based on Repeater Hops												
	1 Hop	2 Hop	3 Hop	4 Hop	1 Hop	2 Hop	3 Hop	4 Hop	1 Hop	2 Hop	3 Hop	4 Hop
Signal	20 MHz Channel				10 MHz Channel				5 MHz Channel			
-72	22	11	5.5	2.8	11.	5.5	2.8	1.4	5.5	2.8	1.4	.7
-75	20	10	5.	2.5	10.	5.	2.5	1.3	5.	2.5	1.3	.6
-81	17	8.5	4.3	2.1	8.5	4.3	2.1	1.1	4.3	2.1	1.1	.5
-84	11	5.5	2.8	1.4	5.5	2.8	1.4	.7	2.8	1.4	.69	.34
-88	9	4.5	2.3	1.1	4.5	2.3	1.1	.6	2.3	1.1	.56	.28
-91	6	3	1.5	.75	3.	1.5	.75	.38	1.5	.75	.38	.19
-91	4.5	2.25	1.1	.56	2.3	1.1	.56	.28	1.1	.56	.28	.14
-92	3	1.5	.8	.38	1.5	.75	.38	.19	.8	.38	.19	.09
-93	1.	.5	.25	.13	0.5	.25	.13	.06	.3	.13	.06	.03

Data Throughput Based on Repeater Hops								
	1 Hop	2 Hop	3 Hop	4 Hop	1 Hop	2 Hop	3 Hop	4 Hop
Signal	2.5 MHz Channel				1.25 MHz Channel			
-72	2.8	1.4	.69	.34	1.4	.69	.34	.17
-75	2.5	1.3	.63	.31	1.3	.63	.31	.16
-81	2.1	1.1	.53	.27	1.1	.53	.27	.13
-84	1.4	.69	.34	.17	.69	.34	.17	.09
-88	1.1	.56	.28	.14	.56	.28	.14	.07
-91	.75	.38	.19	.09	.38	.19	.09	.05
-91	.56	.28	.14	.07	.28	.14	.07	.04
-92	.38	.19	.09	.05	.19	.09	.05	.02
-93	.13	.06	.03	.02	.06	.03	.02	.01

3.2 Configuring the Unit for the First Time

The 945U-E has a built-in Web server, containing webpages for analyzing and modifying the module's configuration. The configuration can be accessed using Microsoft® Internet Explorer® version 7 or greater. This program is shipped with Microsoft Windows® or may be obtained freely via the Microsoft website. If using other browsers, they must be fully compliant with Internet Explorer 7 SSL security.

NOTE Microsoft Internet Explorer Version 6 will not load webpages due to a compatibility issue between IE6 and SSL-security websites.

Default Configuration

The default factory configuration of the 945U-E is as follows:

- Client/Bridge.
- IP address 192.168.0.1XX, where "XX" is the last two digits of the serial number (the default IP address is shown on the printed label on the back of the module).
- Netmask 255.255.255.0.
- Username is "user" and the default password is "user".

The 945U-E will temporarily load some factory default settings if powered up with the factory default switch (on the end-plate of the module) in the SETUP position. When in SETUP mode, wireless operation is disabled. The previous configuration remains stored in non-volatile memory and will only change if a configuration parameter is modified and the change saved.

NOTE Remember to set the switch back to the RUN position and cycle power at the conclusion of configuration for resumption of normal operation.

Accessing Configuration for the First Time

Because the default IP address of the 945U-E is within the range 192.168.0.XXX, the module may not connect to your network or PC. There are two methods for accessing the configuration for the first time.

METHOD 1: Change your computer settings so that the configuring PC is on the same network as the 945U-E with the factory default settings. This is the preferred method and is much simpler than the second method. You will need a straight-through Ethernet cable between the PC Ethernet port and the 945U-E. The factory default Ethernet address for the 945U-E is 192.168.0.1XX, where "XX" is the last two digits of the serial number (check the label on the back of the module).

METHOD 2: Requires temporarily changing the IP address in the 945U-E via an RS232 connection so that it is accessible on your network without having to change your PC network settings. When connected you can change the modem network settings to match that of your network.

Method 1 – Set PC to Same Network as 945U-E

1. Connect the Ethernet cable between module and the PC configuring the module.
2. Set the factory default switch to the SETUP position.

   This will always start the 945U-E with Ethernet IP address 192.168.0.1XX, subnet mask 255.255.255.0, gateway IP 192.168.0.1, and the radio disabled.

   NOTE Remember to set the switch back to the RUN position and restart the module at the conclusion of configuration for resumption of normal operation.
3. Power up the 945U-E module.
4. On the PC, open the Control Panel, and then open **Network Settings**.

   The following description is for Windows XP. Earlier Windows operating systems have similar settings.
5. Open **Properties** of Local Area Connection.

6. Select **Internet Protocol (TCP/IP)** and click **Properties**.

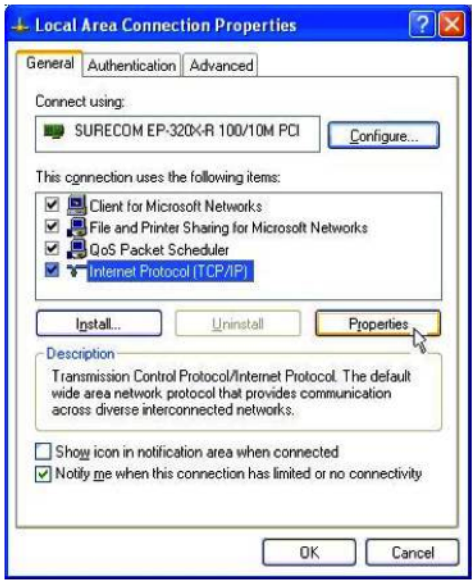


Figure 19 Local Area Connection

7. On the **General** tab, enter IP address 192.168.0.1, subnet mask 255.255.255.0 and click **OK**.

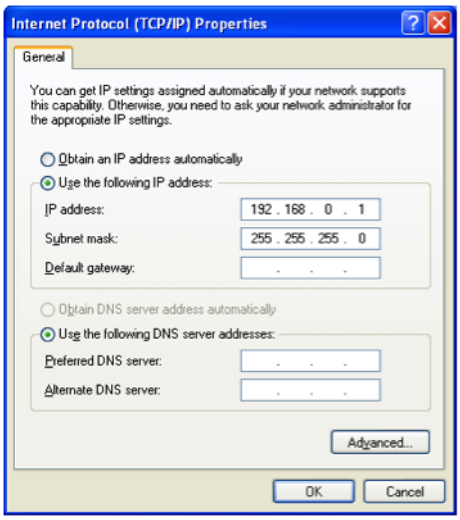


Figure 20 TCP/IP Properties

8. Open Internet Explorer and ensure that settings will allow you to connect to the IP address selected.

   If the PC uses a proxy server, ensure that Internet Explorer will bypass the proxy server for local addresses.

   This option may be modified by opening Tools -> Internet Options -> Connections Tab -> LAN Settings->Proxy Server -> bypass proxy for local addresses.

9. Enter the default IP address for the 945U-E.

   The default address is 192.168.0.1XX, where “XX” is the last two digits of the serial number.

10. Enter the username “user” and default password “user.”

Figure 21 Main Screen

11. To resume normal configured operation when configuration is complete, switch the factory default DIP switch on the 945U-E to RUN and cycle power.

NOTE Security Certificates. Configuration of the 945U-E uses an encrypted link (https). The security certificate used by the 945U-E is issued by ELPRO and matches the IP address 192.168.0.100.

When you first connect to the 945U-E, your Web browser will issue a warning that ELPRO is not a trusted authority. Ignore this warning and proceed to the configuration webpage.

Internet Explorer 7 has an additional address check on security certificates. Unless the 945U-E has the address 192.168.0.100, when you first connect to the 945U-E Internet Explorer 7 will issue a warning about mismatched security certificate address. You can turn off this behavior in IE7 by selecting:

Tools > Internet Options > Advanced > Security > Warn about certificate address mismatch

Method 2 – Set 945U-E Network Address to Match the Local Network

For this method you will need to determine what IP address, Gateway address, and netmask to assign to the 945U-E so that it appears on your network. Ask your system administrator if you do not know the correct settings for your network. The default IP address of the 945U-E modem is 192.168.0.1 and the network you wish to connect to is on 10.10.0.X (the PC is on 10.10.0.5).

Once you have determined the correct settings for your network, you need to connect to the modem's RS-232 serial port using a straight-through serial cable and a terminal package (such as HyperTerminal) set to 115,200 baud. 8 data bits, 1 stop bit, no parity.

1. Open HyperTerminal and monitor communications.
2. Set the SETUP/RUN switch to the SETUP position, and connect power to the modem.
3. Observe HyperTerminal and when you see the ELPRO Dragon screen (see Figure 22) press **Enter** to get the prompt "#."
4. Type the following "ifconfig" command to show the configuration of the Ethernet port. From this you will be able to see the IP address.

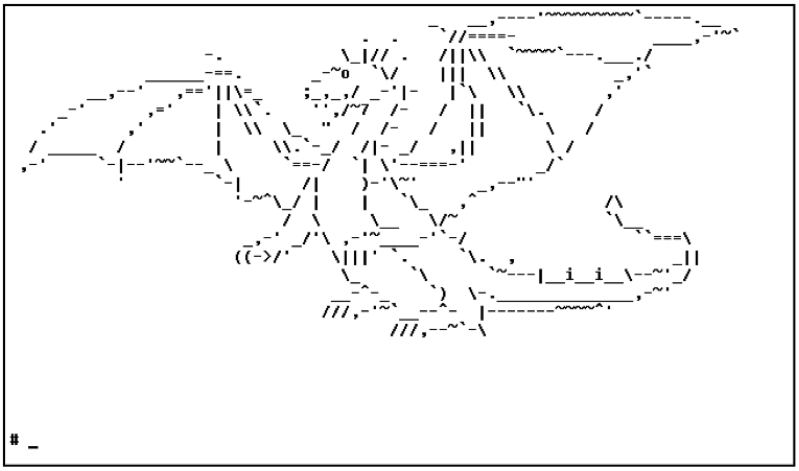


Figure 22 Dragon

eth0 Link encap:Ethernet HWaddr 00:12:AF:FF:FF:FF

inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0

UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1

RX packets:8 errors:0 dropped:0 overruns:0 frame:0

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:256

5. Temporarily change the IP address to an one that will enable connection to your local network.

   For example, type “ifconfig eth0 10.10.0.6 netmask 255.255.255.0”. Only add the netmask if the netmask is anything other than the standard 255.255.255.0.

   IP address should now be changed.

6. Verify that the IP address is changed by typing “ifconfig” again.

   Note that these changes are only temporary, and if the module is reset they will go back to the normal default (192.168.0.XXX).

7. Open Internet Explorer and ensure that settings will allow you to connect to the IP address selected. If the PC uses a proxy server, ensure that Internet Explorer will bypass the proxy server for local addresses.

   This option may be modified by opening Tools -> Internet Options -> Connections Tab -> LAN Settings->Proxy Server -> bypass proxy for local addresses.

8. Enter the IP address for the 945U-E into the Internet Explorer address bar.

   For example, if you changed the temporary address in step 5 to “10.10.0.6,” you would enter http://10.10.0.6.

9. Enter the username “user” and default password “user.”

   You should now be connected to the main index page on the modem.

10. Connect to the Network page and change the Ethernet Interface and Wireless Interface IP addresses to 10.10.0.6.

11. Switch the RUN/SETUP switch back to RUN and click **Save Changes and Reset**.

NOTE Because the modem can be setup numerous ways (such as a bridge or router), this setup will allow the modem to appear on the 10.10.0.X network. Any other configuration changes can be made after this initial connection (see the following sections on configuration).

3.3 Quick Start

The 945U-E has a Quick Start Configuration option that covers the most important parameters needed to get an initial connection. This is the first stage of the module configuration. For most applications, no further configuration is required. For more advanced applications, additional parameters can be changed via the normal configuration pages after the Quick Start configuration has been saved.

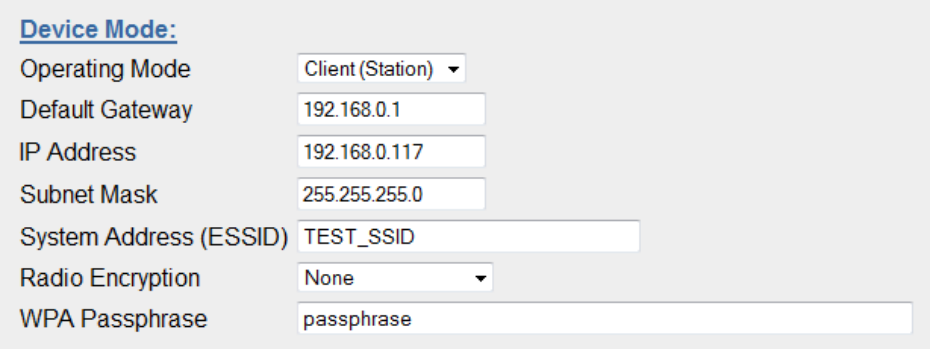


Figure 23 Quick Start

Quick Start Configuration:

1. Select **Quick Start** from the Main Menu, and then set the following parameters:

   - **Operating Mode**—Access Point or Client. Bridge operation is assumed. For router selection, go to the Network page after Quick Start.
   - **Default Gateway**—This is the address that the device will use to forward messages to remote hosts that are not connected to any of the local bridged networks (Ethernet or Wireless).
   - **IP Address / Subnet Mask IP**—IP address and subnet mask for your application.
   - **System Address (ESSID)**—The system address is a text string 1 to 31 characters long used to identify your system.
   - **Radio Encryption**—Radio encryption selection (None, WPA-PSK (TKIP), WPA-PSK (AES) or WPA2). Refer to "3.7 Security Menu" if WEP or enterprise encryption is required.
   - **WPA Passphrase**—128-bit encryption keys are internally generated based on the passphrase and system address (ESSID). The passphrase must be between 8 and 63 characters long, and must be the same for all 945U-E units in the same system.

   The default settings will be shown. If your system is connecting individual devices that are not connected to an existing Ethernet LAN, you can use the factory default IP values. If you are connecting to an existing LAN, you need to change the IP addresses to match your LAN addresses.

2. After configuring, click **Save to Flash and Reset**.

   Radio Data Rate and Channel will be set to "Auto," Radio Transmit Power will be set to maximum, and any previous configuration of unrelated parameters will not be modified and will still apply.

3.4 Network Configuration

You can view or modify Ethernet network parameters by selecting the Network menu. When prompted for the username and password, enter “user” as the username, and “user” as the password. This is the factory default setting. To change the default username and password, see “3.23 Module Information Configuration.” If you have forgotten the IP address or password, the factory default switch may be used to access the existing configuration. Refer to the previous section for more information.

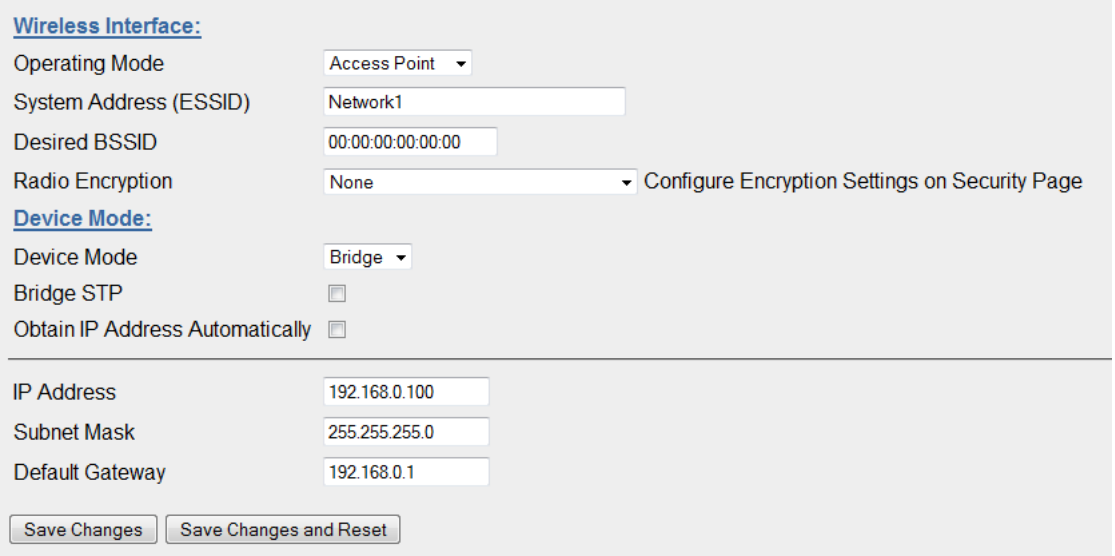


Figure 24 Network

The Network Configuration page allows configuration of parameters related to the wired and wireless Ethernet interfaces. In general, IP address selection will be dependent upon the connected wired Ethernet device(s). Before connecting to an existing LAN consult the network administrator.

Default configuration of the module will be “Client” and “Bridge.” When in Bridged mode the module’s wired and wireless IP address will be the same, meaning only one IP address is required. If the device mode is changed to “Router” the page will display two IP addresses, one for Ethernet and one for wireless. For more information on bridging networks, see “3.18 Routing.”

If the module has been configured for VLAN, the page will show device mode as “VLAN Bridge,” and the Ethernet IP and netmask will no longer be editable. See “3.22 VLAN” for details on VLAN configuration.

A system of 945U-Es must have at least one access point, configured as a master, and have one or more clients. All 945U-Es should be given the same system address (ESSID) and radio encryption settings. For further information and examples on wireless network topologies refer to “1.0 Network Topology.”

The 945U-E supports several different radio encryption schemes. If utilizing any form of encryption, all modules in the system that communicate with each other will need the same encryption method and encryption keys.

The available encryption methods are as follows:

- **WEP (Wired Equivalent Privacy)** encryption is the weakest encryption method defined by the original IEEE802.11 standard and uses a 40-bit or 104-bit key with a 24-bit initialization vector to give a 64-bit and 128-bit WEP encryption level. WEP is not considered an effective security scheme, and should only be used if it is necessary to inter-operate with other equipment which does not support more modern encryption methods.
- **WPA (Wi-Fi Protected Access)** is a subset of the IEEE802.11i Security Enhancements specification.
- **WPA2 (Wi-Fi Protected Access 2)** replaced WPA and provides significant security improvements over this method. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.

- **WPA/WPA2-PSK (Legacy Support)** enables the modem to communicate to all WPA methods including TKIP, AES, and WPA2 AES. Generally only used if the network has older devices that does not support the higher level encryption methods. Enabling this option will lower the security level of the network down to the weakest configured encryption level (WPA TKIP).
- **WPA-Enterprise (802.1x)** removes the need to manage the pre-shared key (PSK) by using an external server to provide client authentication. Clients that are not authorized will be prevented from accessing the network. Once a client has provided the correct authentication credentials, access is permitted and data encryption keys are established, similar to WPA-PSK. Fine grain (user level) access control can be achieved using this method.

  An 802.1x capable RADIUS server may already be deployed in a large scale network environment. The 945U-E can make use of this server reducing replication of user authentication information.

  In a typical WPA-enterprise setup, the 945U-E access point acts as Authenticator, controlling access to the network. Wireless clients (945U-Es, laptops or other devices) act as Supplicants, requesting access to the network. The Authenticator communicates with an authentication (RADIUS) server on the Ethernet network to verify Supplicant identity. When a Supplicant requests access, it sends an access request to the Authenticator, which passes an authentication request to the external authentication server. When the user credentials of the Supplicant are verified, the Authenticator enables network access for the Supplicant, data encryption keys are established and network traffic can pass.

  Configuration of WPA-enterprise differs when the unit is configured as an access point (Authenticator) or client (Supplicant). If WDS interfaces are used, it is possible for one 945U-E to act as both an Authenticator and a Supplicant, but in this situation only one set of user credentials can be entered for all Supplicants.

  The 945U-E supports WPA-1 TKIP, WPA-1 AES and WPA-2 AES using a pre-shared key (PSK).
- **WPA PSK TKIP** (Temporal Key Integrity Protocol) enhances WEP by using 128-bit encryption plus separate 64-bit TX and RX MIC (message integrity check) keys.
- **WPA PSK AES** (Advanced Encryption Standard) uses the more advanced CCMP encryption protocol and is essentially a draft of the IEEE 802.11i wireless network standard. This is the recommended encryption method for most applications.
- **WPA2 AES** (Advanced Encryption Standard) is the most secure encryption method and is also based on 128-bit encryption key.

After changes are made to Network Configuration, it is important to save the configuration by clicking Save Changes or by clicking Save Changes and Reset.

NOTE If making changes to a remote module via the radio link, make sure all changes are compliant and accurate before clicking Save to Flash and Reset. Some field changes may stop the radio link from working and will require a hard wire connection to restore.

Network Settings Webpage Fields

Operating Mode	Used to select Access Point (Infrastructure), Client (Infrastructure). By default this is set to Client.
System Address (ESSID)	A 945U-E wireless network comprises modules with the same system address. Only modules with the same system address will communicate with each other. The system address is a text string 1–31 characters long. Select a text string that identifies your system.
Desired BSSID	To force a client/station to always connect to the same access point, enter the MAC address of that access point in the Desired BSSID field. Note that the ESSID of the access point must also match the configured ESSID of the client.
Radio Encryption	Select the desired radio encryption level. The encryption key, passphrase, and other security information is entered on the Security Menu. See “3.6 Security Menu.”

Device Mode	Used to select Bridge or Router mode. By default, this is set to Bridge. If VLAN is enabled the Device Mode will indicate “VLAN” and the IP Address and Netmask will only be editable from the VLAN page.
Bridge STP	Selecting this checkbox enables Spanning Tree Protocol in bridged networks. See “3.5 Spanning Tree Algorithm” for details.
Obtain IP Address Automatically	Selecting this checkbox enables DHCP client on the 945U-E. A DHCP client requests its IP address from a DHCP server which assigns the IP address automatically. For more information, refer to “3.20 DHCP Server Configuration.” By default, this option is not selected.
IP Address	Bridge Mode—The IP address of the 945U-E module. Both wired (Ethernet Interface) port and wireless (Wireless Interface) ports will take on this address. Router Mode—Separate IP addresses are required for each interface. IP addresses must be different.
IP Subnet Mask	The IP network mask of the 945U-E module. This should be set to the appropriate subnet mask for your system (typically, 255.255.255.0). In Router mode, each interface will have its own netmask.
Default Gateway	This is the address that the device will use to forward messages to remote hosts that are not connected to any of the local bridged networks (Ethernet or Wireless). This is only required if the wired LAN has a gateway unit that connects to devices beyond the LAN (for example, Internet access). If there is no gateway on the LAN, set this to the same address as the access point (the Ethernet IP Address below). Refer to “3.17 Routing Rules” for more information.
Save Changes	Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.
Save Changes and Reset	Save settings to non-volatile memory and reboot the 945U-E. Once the module has completed the reboot sequence, all changes are in effect.

3.5 Spanning Tree Algorithm

The bridge Spanning Tree Protocol (STP) function was introduced to handle network loops and provide redundant paths in networks. To enable this function, select the STP checkbox on any WDS connections that you have configured on the Repeaters configuration page.

For example, consider the following network (Figure 25) with a redundant wireless link. If the bridge STP is enabled, one of the two wireless links will be disabled and all wireless data will be transferred by one link only. If the active link fails, the other link will automatically start transferring the wireless data.

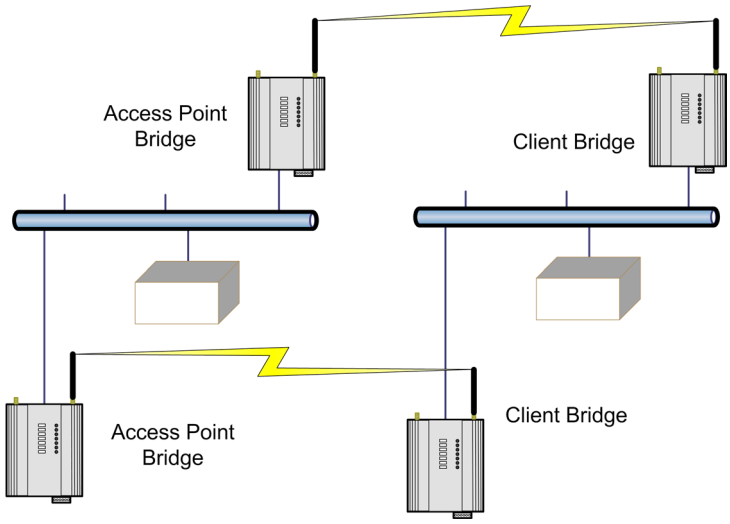


Figure 25 Spanning Tree Protocol

The STP implemented is IEEE 802.1d compatible. The algorithm forms a loop-free network by blocking traffic between redundant links in the network. These blocked links are placed in a standby condition and may be automatically enabled to repair the network if another link is lost.

The spanning tree algorithm maintains a single path between all nodes in a network by forming a tree-like structure. The bridge priority determines where the node sits in the tree. A bridge configured with the lowest priority (0) will become the root node in the network, and will direct traffic between each of its branches. The root node is typically the unit that handles the majority of traffic in the network. Buy default, the 945U-E is configured with a bridge priority of 32768. The intention is to reduce traffic that the 945U-E must handle by placing it at the branch level in the network tree. As a branch, the 945U-E need only pass traffic to devices that are its leaf nodes.

There is some overhead in maintaining a network utilizing the spanning tree algorithm. Users wishing to increase their throughput at the expense of redundancy should disable Spanning Tree. STP can be configured on the Repeaters configuration page.

3.6 Security Menu

Select the Radio Encryption level from the drop down menu on the main index page, and then click Save Changes. Available encryption levels are None, WEP (64-bit), WEP (128-bit), WPA PSK (TKIP), WPA PSK (AES), WPA2 PSK (AES), WPA PSK/ WPA2 PSK (Legacy), and WPA-Enterprise. The default setting is “None.”

you will now need to go to the Security Menu and enter the encryption keys (WEP), passphrase (WPA).

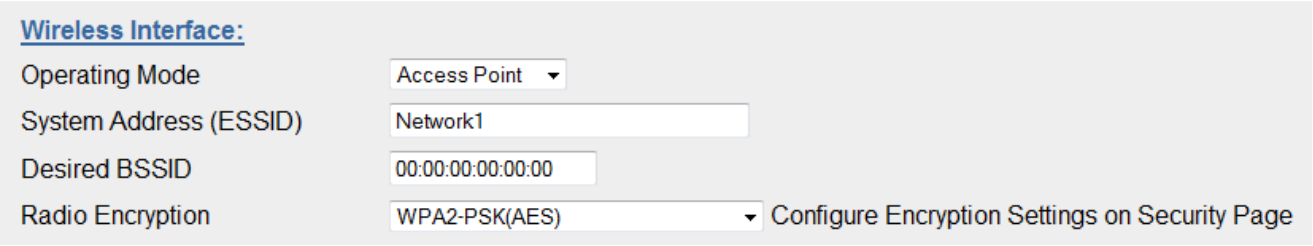


Figure 26 Security Menu

WEP (64 bit) and (128 bit)

Encryption Keys 1 to 4

These are the keys used to encrypt radio data to protect data from unwanted eavesdroppers when WEP Encryption is selected. These keys should be the same for all 945U-E units in the same system. WEP keys must be entered as pairs of hexadecimal digits separated by colons. Hexadecimal digits are in the range 0...9 and A...F.

The 64-bit WEP requires 10 hexadecimal digits, and 128-bit WEP requires 26 hexadecimal digits. For example, 12:AB:EF:00:56 for 64-bit encryption, and 12:AB:EF:00:56:15:6B:E4:30:C8:05:F0:8D for 128-bit encryption.

Encryption keys must not be all zeros (00:00:00:00:00).

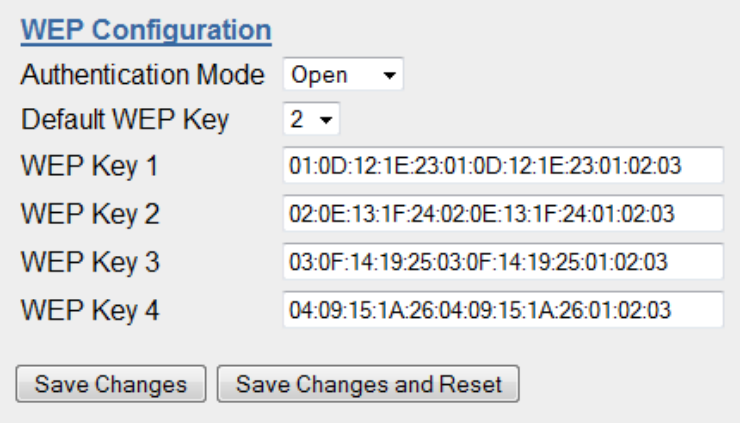


Figure 27 WEP

Default WEP Key

One of the four keys may be selected as the default key and is used to encrypt transmitted messages from the configured unit. A 945U-E can receive and decrypt a message from a module that has a different default key index as long as each module has the same key configured at the same index.

WEP Open Authentication Mode

- Station sends an authentication request to the access point.
- Access point then authenticates the station.
- Station then associates with the access point and joins the network.

WEP Shares Authentication Mode

- Station sends an authentication request to the access point.
- Access point then sends a text-based message to the station.
- Station uses its own WEP key to encrypt the text-based message and sends it back to the access point.
- Access point then decrypts the message using its on WEP key and if the key matches it authenticates the station.
- Station then associates with the access point and joins the network.

WPA / WPA2

When WPA encryption is selected, 128-bit encryption keys are internally generated based on the passphrase and system address (ESSID). The passphrase must be between 8 and 63 characters long, and the passphrase must be the same for all 945U-E units in the same system.

For optimal security consider using a passphrase consisting of a combination of letters and numbers (not just a simple word or phrase), as well as upper and lowercase. For example, “WiReLeSs TeChNoLoGy 2010.”

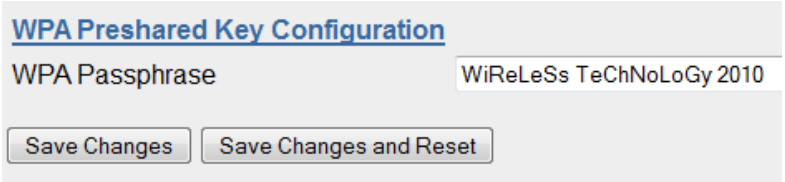


Figure 28 WPA

WPA Enterprise - Authenticator (AP) Configuration

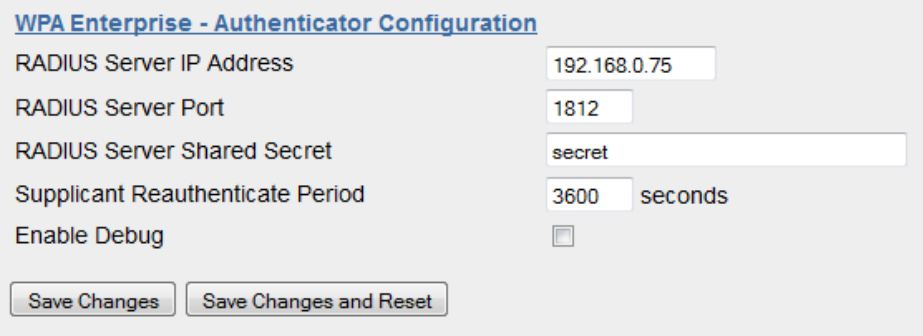


Figure 29 WPA Enterprise Authenticator

RADIUS Server IP Address/Port/shared secret	Connection information for the RADIUS authentication server.
Supplicant Reauthenticate Period	Sets the maximum time at which the Supplicant must re-authenticate. This parameter determines maximum time a client will have access to the network after its user credentials have been revoked.
Enable Debug	Must only be used during commissioning and only if requested by ELPRO technical support. This must be disabled for normal operation.

WPA Enterprise - Supplicant (Client) Configuration

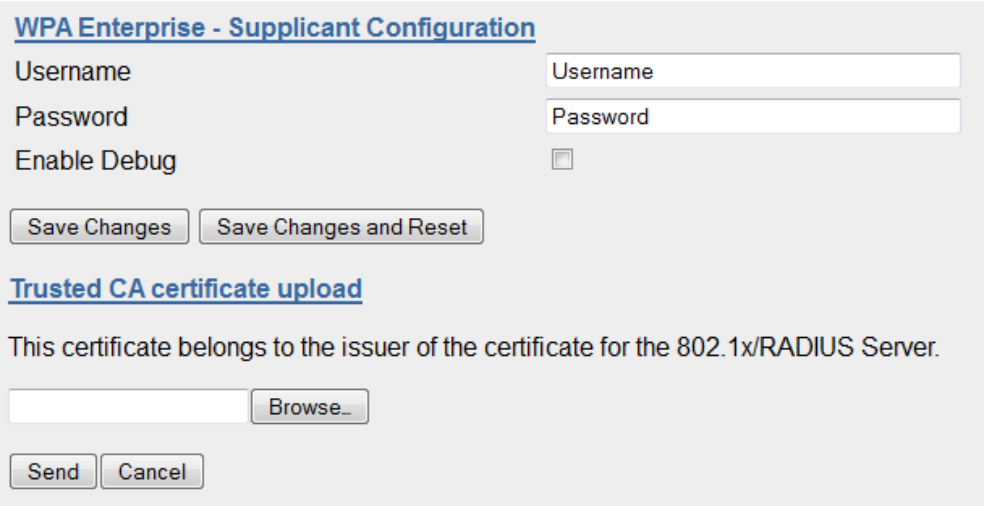


Figure 30 WPA Enterprise Supplicant

Username / Password	User credentials that match a valid user on the RADIUS server.
Enable Debug	Disabled for normal operation. Enables debug mode for use during commissioning. To be used only if requested by ELPRO technical support.
Trusted CA certificate upload	Upload the certificate of the issuer of the RADIUS server's certificate. This enables the Supplicant to verify the identity of the RADIUS server during the authentication process. Supported EAP method is PEAP / MSCHAPv2.
Certificate Verification result	Once a certificate has been loaded, this field will contain validation information for the certificate. If this field is blank or contains errors, the certificate is invalid.
Trusted CA Certificate Contents	Displays the contents of the loaded certificate.

3.7 Normal Operation

After addresses are configured the units are ready for operation. Refer to "1.0 Network Topology" for an explanation on the operation of a bridge and router.

Bridge Operation (Transparent Network)

A bridge connects several Ethernet networks together, and makes them appear as a single Ethernet network to higher protocol layers. By default, the 945U-E is configured as a transparent bridge. When a transparent bridge is started, it learns the location of other devices by monitoring the source address of all incoming traffic. Initially it forwards all traffic between the wired Ethernet port and the wireless port. However, by keeping a list of devices heard on each port the transparent bridge can decide which traffic must be forwarded between ports and will only transfer a message from the wired port to the wireless port if it is required.

A bridge will forward all broadcast traffic between the wired and wireless ports. If the wired network is busy with broadcast traffic, the radio network on the 945U-E can be unnecessarily overburdened. Use filtering to reduce broadcast traffic sent over the radio. Refer to "3.18 Filtering" for information on how to configure a filter.

By default, a transparent bridge does not handle loops within the network. There must be a single path to each device on the network. Loops in the network will cause the same data to be continually passed around that loop. Redundant wireless links may be set up by enabling the bridge Spanning Tree Protocol (see "3.5 Spanning Tree Algorithm" for details).

Router Operation (Routed Network)

A router joins separate IP sub-networks together. The router has different IP addresses on its wired and wireless ports, reflecting the different IP addresses of the separate Ethernet networks. All of the devices in these separate networks identify the router by IP address as their gateway to the other network. When devices on one network wish to communicate with devices on the other network, they direct their packets to the router for forwarding.

Because the router has an IP address on each of the networks it joins, it inherently knows the packet identity. If the traffic directed at the router cannot be identified for any of the networks to which it is connected, the router must consult its routing rules as to where to direct the traffic. For details on configuring routing rules, see “3.17 Routing Rules.”

3.8 Radio Configuration

The 945U-E can be configured for different radio transmission rates. A reduction in rate increases the reliable range (transmission distance). The factory default data rate settings are suitable for the majority of applications and should only be modified by experienced users.

The 945U-E allows for a configurable fixed rate or an “Auto” radio transmission rate. When a fixed rate is configured, the radio transmission rate is never altered even under extremely poor conditions. When Auto rate is configured, the radio transmission rate will automatically change to give the best throughput. When a radio transmission is unsuccessful the 945U-E will automatically drop to the next lowest data rate, and if subsequent transmissions are successful at the lower rate, the 945U-E will attempt to increase to the next highest rate. When a station connects to an access point, the two devices negotiate a data rate based on which is within the configured range of radio data rates for both devices.

Select the Radio menu to change the following configuration parameters. If a change is made, you need to select Save Changes to retain the changes. Changes will not take effect until the module is reset.

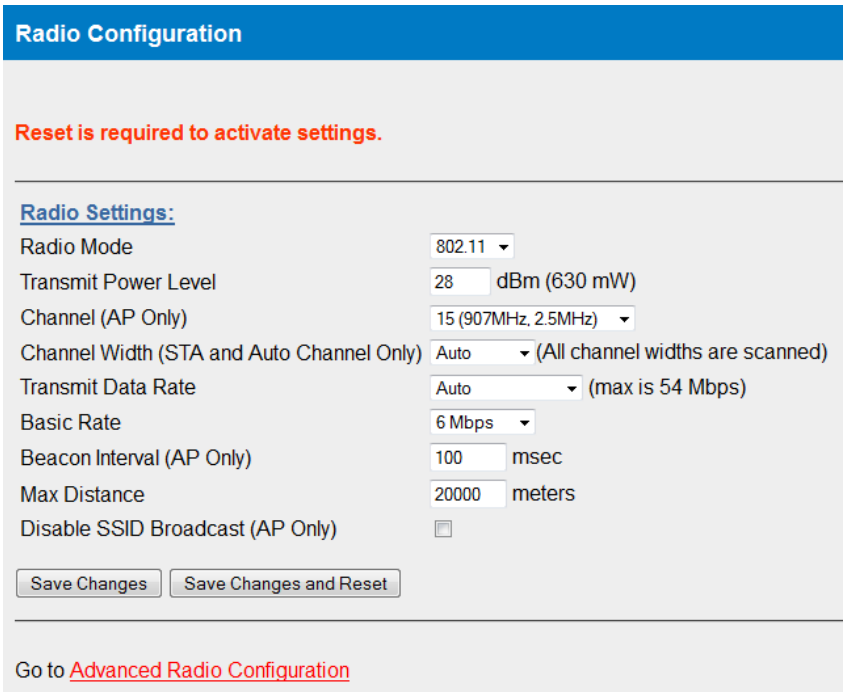


Figure 31 Radio Configuration

Radio Mode	The 945U-E only supports the 802.11 standard.
Transmit Power Level	This allows adjustment of the radio power. Do not set the radio power above the allowed setting for your country You can reduce the power for short range applications, or to allow the use of high gain transmitter antennas while still complying with the emission requirements of your country. See “Appendix C - POWER CONVERSION” for dBm to mW conversion.
Channel (AP Only)	Select available channel, frequency and bandwidth from drop down list. Different regions will show the channels available for that region.
Channel Width	Used when configuring clients (STA). A Client will scan for available access points that it can then connect with. Selecting a Channel Width will limit the number of channels the client will scan. For example, if “5 MHz” is selected the client will only scan the 5-MHz channels. If “Auto” is selected, it will scan all channels and all bands (default is Auto).
Transmit Data Rate	The radio baud rate in Mega (million) bits per second (Mbps) for point-to-point radio transmissions. The default value is Auto. Select a fixed rate to force the radio to use the selected rate. **NOTE Fixing the TX Rate is not recommended except for advanced users. The Transmit Data Rate only applies to the transmit messages; the radio can receive on all data rates.** Increasing the Transmit Data rate will decrease the transmit power level. For example, a 36-Mbps data rate will reduce the TX power to 400 mW, a 48-Mbps data rate will reduce the power to 200 mW, and 54-Mbps data rate will reduce the power to 125 mW.
Basic Rate	This is the default data rate that the access point uses when sending beacons, management frames, and all broadcast or multicast frames.
Beacon Interval (AP only)	This interval is the period between beacon transmissions sent by an access point. The default value is 100 milliseconds, and it may be adjusted from 50 to 4095 milliseconds.
Max Distance	Configure the maximum distance the radio signal is expected to travel. This allows the modem to compensate for the flight time of messages as they pass from the transmitter to the receiver, and as the acknowledgment messages are returned. Setting this value larger will cause a small reduction in throughput. Setting this value too small will cause communications problems over longer distances. Default distance is 20 km.
Disable SSID broadcast (AP only)	This should be used to prevent unwanted eavesdroppers from detecting the radio network system address (SSID) by passively listening to beacon transmissions from the access point. When disabled, access points will not transmit the system address openly in beacon messages. This is particularly useful in unencrypted radio networks.
Save Changes	Save changes to non-volatile memory. Changes will not take effect until module is reset.
Save Changes and Reset	Save changes to non-volatile memory and reset module.

Channel Selection

945U-E (900MHz 802.11) channel selection is performed by selecting the appropriate channel from the drop down list. Only channels available for that region will be available.

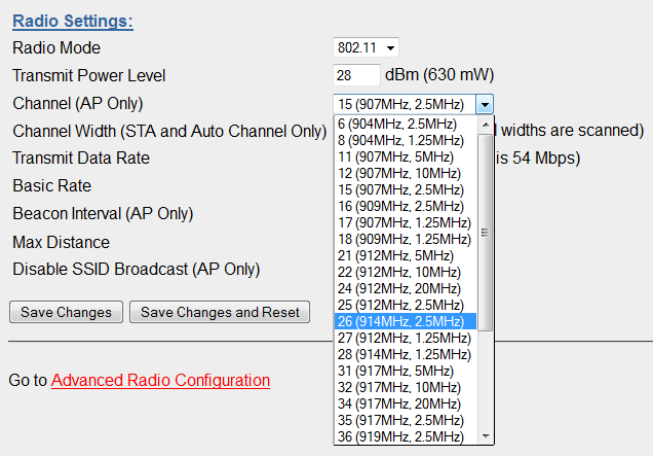


Figure 32 US/Canadian Channels

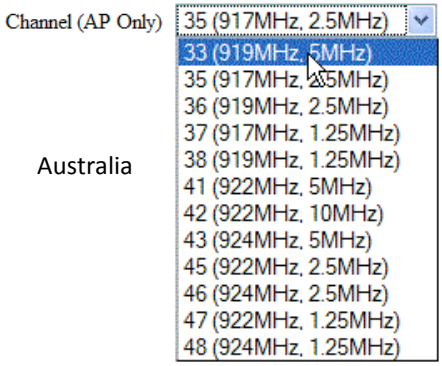


Figure 33 Australian Channels

3.9 Advanced Radio Configuration

Some of the more advanced radio settings have been moved from the normal Radio configuration page to the Advanced Radio Settings page to simplify the configuration process. Care should be taken when making changes to parameters on this page.

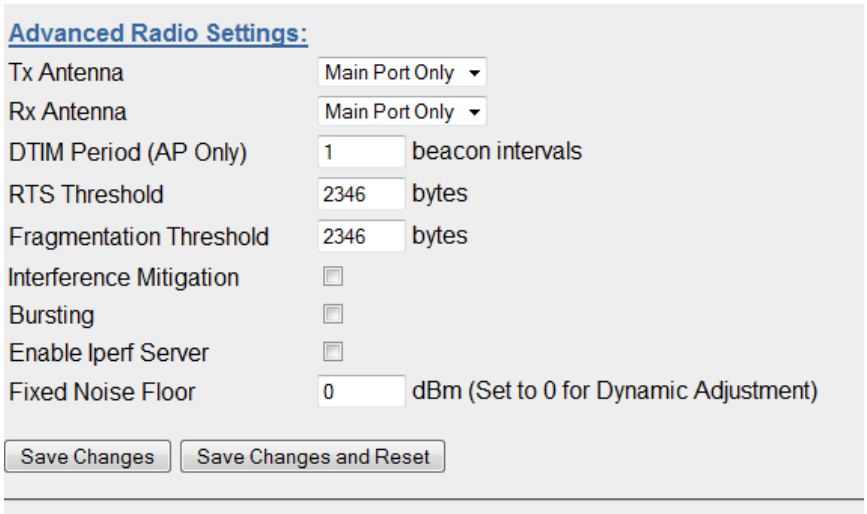


Figure 34 Advanced Radio Settings

TX Antenna	Select which antenna port the module will transmit from: **Main Port Only**—Messages are transmitted from the main TX/RX port. The auxiliary port RX is disabled. **Both (Diversity)**—Both ports will be used to transmit, but not at the same time. It calculates the best port based on previous transmissions and MAC addressing. ⚠ **NOTE Broadcast / UDP transmission messages will initially toggle between the antenna ports, and could result in every second message not being heard until the module learns which device can be reached through which antenna port.** **Aux Port Only**—Messages will be transmitted via the auxiliary RX port only.
RX Antenna	Same as for TX antenna above, but for the receiver port. Setting to "Both (Diversity)" will allow a high gain antenna to be connected to the auxiliary "RX" port, which will give better RX signal gain without increasing the TX gain and possibly pushing it over the regulatory EIRP threshold.
DTIM Period	(Access point only.) DTIM sets which beacon frames incorporate extra information for low power sleeping client devices. Normally set this to 1.
RTS Threshold	Request To Send threshold. RTS frames can be used to help avoid radio collisions between two stations that cannot directly hear each other. Any frame larger than the RTS threshold bytes will be preceded by an RTS message. The default value of RTS threshold is 2346, which effectively disables RTS signaling, as this value is larger than the maximum frame size (fragmentation threshold).
Fragmentation Threshold	(Client stations only.) The maximum transmission unit (MTU) of data over the radio. If more than this number of bytes is input into the module, it will be transmitted in more than one message (fragmented).
Interference Mitigation	(Access point only.) Interference Mitigation should only be turn on (default is Off) if using demo whip antennas, or if there is a high level of background interference. By enabling this option, the radio will dynamically adjust radio parameters to help mitigate interference based on any background interference. It will reduce the receiver sensitivity and therefore should only be enabled on paths with a high fade margin and good signal quality.
Bursting	Selecting this option can increase the data throughput by reducing the overheads associated with wireless transmissions.
Enable Iperf Server	Enable Iperf Server function in the modem. Iperf is used for performing radio surveys or radio path testing. See "4.4 Throughput Test."
Fixed Noise Floor	Allows the radio receiver noise floor (and therefore sensitivity) to be moved above any interference. This essentially stops the radio from communicating with devices that have lower signal strength. For use in areas where there is a greater amount of interference.

Fixed Noise Floor

900MHz FHSS band can have many sources of interference. This interference can sometimes be a problem due to the way 802.11 devices communicate. Standard 802.11 communications uses a system called "clear channel assessment" which means the radio will listen before transmission and if the channel is busy it will hold off regardless of the level of signal. If the background interference is high due to other radio systems or noise, you can raise the fixed noise floor to compensate. The Channel Utilization page can be used to identify excess noise or interference.

Raising the noise floor will block out any receive signal levels below the value configured under "Fixed Noise Floor" on the Advanced Radio Configuration page. The value must be entered as a negative dBm number and should be at least 8 dB greater than the weakest RSSI of any connected modems, otherwise communications may be lost.

For example, if the interfering noise levels are around -80 dB you can raise the noise floor to -70 dB to block out any signals below, making sure that the RSSI levels of any connected modules are not below this noise floor as they will not communicate. The Connectivity page can be used to determine if other systems are in the area and their RSSI levels.

After configuring the fixed noise floor, confirm that the channel utilization has dropped to a desirable level and where possible perform an Iperf throughput test to confirm acceptable performance.

3.10 Serial Port Configuration

The 945U-E has an RS-232 and an RS-485 port for serial communications. These ports may be used for different purposes. The 945U-E offers three serial functions—PPP server, serial gateway, and Modbus TCP to RTU gateway.

RS-232 PPP Server

The 945U-E can be used as a PPP (Point-to-Point Protocol) server to connect the wireless system to serial devices via the RS232 or RS485 serial ports. PPP server enables a network connection to the 945U-E over a serial cable. This is much like dial up Internet. The maximum serial data rate is 115,200 bps. Hardware or software flow control may be selected. With minimal configuration on the PC, you may use dial-up networking in Windows XP to connect to the network via the serial port.

For the 945U-E, users must configure the local IP address for the 945U-E and the remote device IP address. Some care must be taken in selecting these IP addresses.

- If you want to use routing over this serial network connection, the IP addresses selected must not lie on wireless or wired Ethernet networks already configured into the device. You must ensure they set routing rules appropriately for devices either side of the network.
- If you want the serial device visible as present on the wireless or wired network, then the local IP address must be the same as the IP address set for the desired port. A process called “proxy ARP” is used to make the device visible on the network. In this process, the 945U-E pretends that it holds the IP address on the network, and responds on behalf of the remote device.

The result of this is similar to bridging for a single device, with some exceptions. One of these exceptions is the inability to handle name server searches of the network via this serial link. For example, you would encounter difficulty if you were to use Windows Explorer over the serial link to find a PC on the wired network. For this to operate correctly you must explicitly map computer names to IP addresses in the LMHOSTS file on your PC.

To configure Windows XP to establish a PPP connection to a 945U-E in SETUP mode:

1. On **Network Connections**, select “Create a new connection.”
2. In the New Connection Wizard, click **Next**.
3. Set up an advanced connection.
4. Connect directly to another computer.
5. Set the PC as guest.
6. Set the Connection Name.
7. Select a COM port.
8. Select availability.
9. Click **Finish**.
10. Select properties of this new connection by right-clicking the connection.
11. On the **General Tab** click **Configure**.
12. Ensure that the maximum speed is 115200 bps, and click **OK**.
13. Select the **Networking Tab**, and then click **Internet Protocol (TCP/IP)** in the list box and click **Properties**

button.

14. On **Properties**, click **Advanced**.
15. On the **Advanced TCP/IP Settings General** tab, clear the field in the PPP link “Use IP header compression.”

    Configuration is now complete.
16. Click the newly created link to establish a connection to 945U-E.
17. Ensure that the username and the password are entered exactly as configured in 945U-E.

    When booted in SETUP mode, the PPP server has the username “user” and password “user.”

Serial Gateway (Server/Client/Multicast)

Serial gateway functionality is available for both RS-232 and RS-485 ports independently, and enables serial data to be routed via the wired or wireless network connection. Serial gateway functionality is similar to radio modem functionality, allowing point-to-point and multipoint serial data transfer.

The serial gateway can be configured as either server, client, multicast group, or Modbus.

- **Server**—When configured as server, the module will wait for a TCP connection to be initiated by a remote client.
- **Client**—When configured as client, the module will automatically attempt to connect to a specified remote server using TCP.
- **Multicast Group**—When configured as multicast group, the module will broadcast data to all members of the same multicast group using UDP.

With the serial gateway server, client, and multicast functions, it is possible for serial data from a 945U-E to be transferred to any other 945U-E serial ports including the corresponding port on the same 945U-E.

Serial Gateway (Modbus–Modbus RTU to TCP)

When configured as Modbus, the module will allow a serial Modbus RTU client (master) to connect with a single Ethernet Modbus TCP server (slave). With the Modbus function, the serial data is encapsulated within a TCP/IP data frame and made available on the Ethernet network. Both 945U-E serial ports and the hard wired Ethernet port can be configured to communicate completely separate data streams that can all be communicating at the same time.

Some of the possible serial gateway topologies are shown in Figure 35.

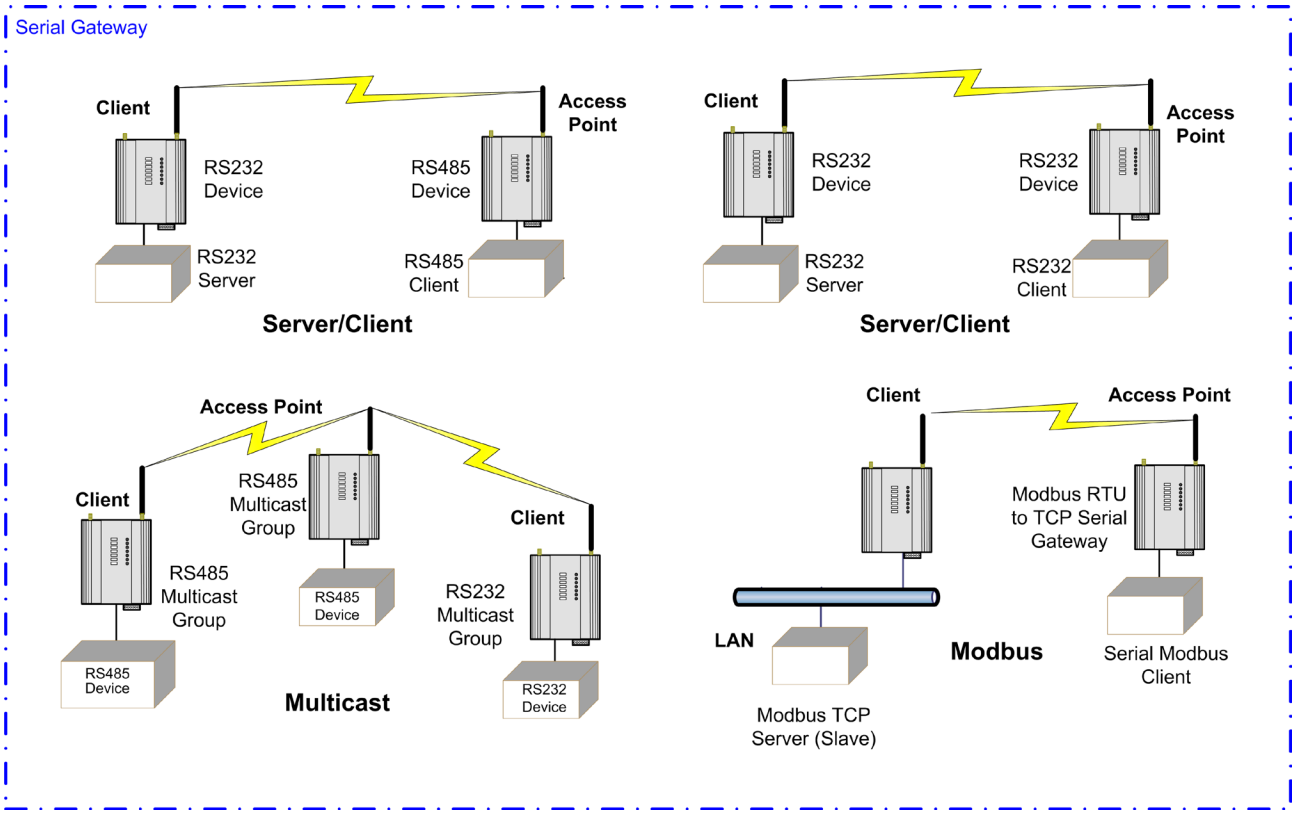


Figure 35 Gateway Topology Examples

There are software packages available (such as SerialIP Redirector by Tactical Software) that can create a virtual serial port on a PC. This virtual serial port can be configured to connect to a 945U-E serial port. Standard programs can then be used to access this serial port as if it were actually connected to the PC. Alternatively, HyperTerminal may be used to connect to a serial port on the 945U-E. When creating the HyperTerminal connection, select "Connect Using: TCP IP (Winsock)," enter the IP address of the 945U-E and the port selected in the "Network Port" field.

Modbus TCP to RTU Gateway

The Modbus TCP to RTU gateway allows an Ethernet Modbus/TCP client (master) to communicate with a serial Modbus RTU slave. The 945U-E makes this possible by internally performing the necessary protocol conversion. Because the conversion is always performed by the 945U-E, which is directly connected to the Modbus serial device, only this module needs to have Modbus TCP to RTU gateway enabled.

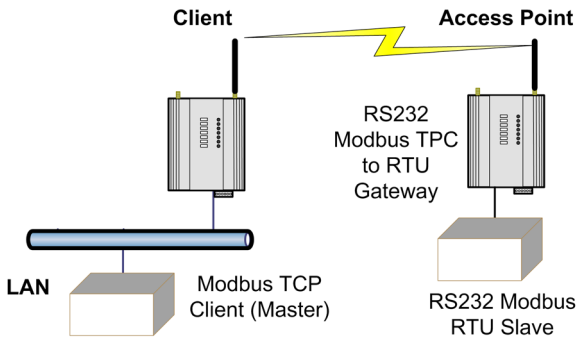


Figure 36 Modbus/TCP Client to Modbus RTU Slaves

The example in Figure 36 demonstrates how a Modbus/TCP client (master) can connect to one or more Modbus RTU (serial) slaves. In this example the 945U-E access point is configured with the “RS232 Modbus/TCP to RTU Gateway” enabled. Once enabled, the gateway converts the Modbus/TCP queries received from the master into Modbus RTU queries and forwards these over the RS232 port to the slave. When the serial response to the query arrives from the slave, it is converted to a Modbus/TCP response and forwarded via the network to the Modbus/TCP master. If no response was received serially by the 945U-E within the configured Response Timeout, the 945U-E will initiate a number of retries specified by the configured Maximum Request Retries.

The Modbus TCP to RTU gateway may be configured to operate on either the RS 232 or RS 485 port.

3.11 Serial Menu

RS-232 / RS485 Serial Port Configuration

RS232 Port	Select the desired functionality. Select either PPP, Serial Gateway or Modbus TCP to RTU.
Data Rate	The serial data rate desired. Serial data rates available range from 110 bps to a maximum of 115,200 bps.
Data Format	The data format desired. All the standard data formats are supported.
Flow Control	Select CTS/RTS or None.

RS232 PPP Server (Only RS232)

Username	User name to enter to access RS-232 PPP server.
Password	Password to access RS-232 PPP server.
Local IP Address	Select the IP address of the PPP server. The remote device may be made visible on the Ethernet or wireless networks by either utilizing proxy-arp or routing. The proxy-arp feature may be enabled by setting the local IP address the same as the Ethernet IP address or the wireless IP address. The module will respond on behalf of the remote device, making it seem like the device is present on the configured network. Alternatively, if the IP address selected is not the same as the Ethernet or wireless IP address, routing is used to pass data to the Ethernet and wireless ports.
Remote Device IP Address	Select the IP address of the remote device. Ensure this address is not the same as any other device on the Ethernet or wireless networks.

RS-232 / RS485 Serial Gateway Mode

Serial Gateway Mode	Server—Module will wait for a connection to be initiated by a remote client.
Character Timeout	Enter the maximum delay (in msec) between received serial characters before the packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Listen Port (Server)	Server only. Enter the TCP port number on which the server must listen for incoming connections. The standard TELNET port is 23.
Serial Gateway Mode	Client—Module will automatically attempt to connect to the specified remote server.
Character Timeout	Enter the maximum delay (in msec) between received serial characters before the packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.

Remote Device Port	Client only. Enter the TCP port number of the remote server (the remote port to automatically connect to).
Remote Device IP Address	Client only. Enter the IP address of the remote server.
Serial Gateway Mode	Multicast—Allows point-to-multi-point serial transfer. All members of the group will receive serial transmissions made by any other member of the multicast group.
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Multicast Group Port	Enter the UDP port number that all members of the group will use. All group members should use the same port number.
Multicast Group IP Address	Enter a valid multicast IP address identifying the group (all group members should use the same multicast group IP address). Valid multicast IP addresses are in the range 224.0.1.0 to 238.255.255.255.
Serial Gateway Mode	Modbus—Allows a serial Modbus client (master) to connect with a single Ethernet Modbus TCP server (slave).
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Modbus Server Port	Enter the TCP port number of the remote server (the remote port to automatically connect to).
Modbus Server IP Address	Enter the IP address of the remote server (the remote IP address to automatically connect to).

RS-232 / RS485 Modbus TCP/RTU Converter

Modbus Server TCP Port	Port number used for the Modbus TCP. Standard port is 502.
Pauses Between Requests	Enter the delay between serial request retries, in milliseconds.
Response Timeout	Enter the serial response timeout, in milliseconds. A serial retry will be sent if a response is not received within this timeout period.
Connection Timeout	Enter the TCP connection timeout, in seconds. If no Modbus/TCP data is received within this timeout period, the TCP connection will be dropped. Set this field to zero for no timeout.
Maximum Request Retries	Enter the maximum number of request retries performed serially.
Maximum Connections	Enter the maximum number of simultaneous TCP connections to the server allowed.

3.12 Multicast Pipe Manager

Previously, it has been difficult to connect a single TCP device (such as a SCADA or DCS system) to multiple remote multicast serial devices. Multicast pipe allows this type of connection. An example would be a SCADA system that needs to communicate with multiple remote serial devices. A modem can be placed at each remote location and connected serially to each device. A multicast pipe is configured to communicate with all devices using a multicast address and port, for example, 224.0.1.1:5000. The SCADA then communicates with the remotes using TCP via the IP address of the multicast manager and the port selected in the configuration, for example, 5001.

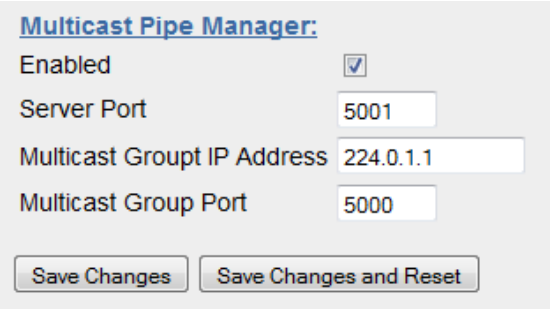


Figure 37 Multicast Pipe

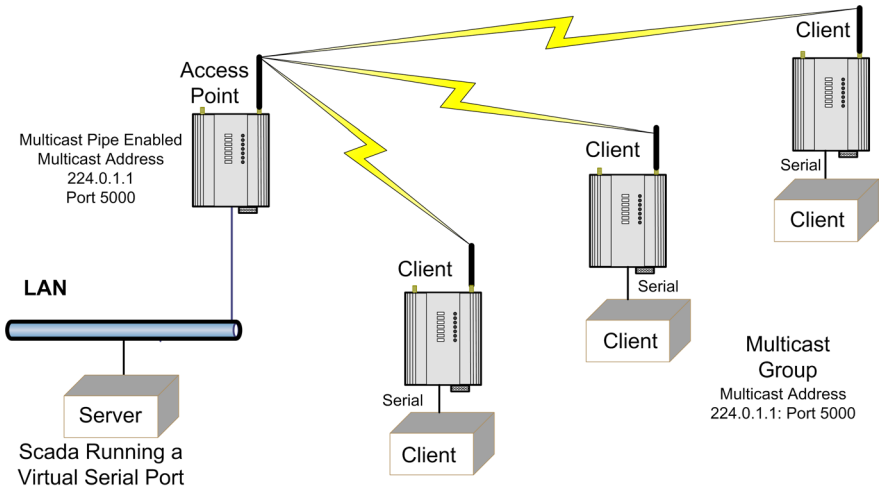


Figure 38 Multicast Group

Enabled	Enables or disables the multicast pipe manager.
Server Port	Server port used by the multicast pipe manager. Will need to be configured the same as the port on the client (for example, SCADA or DCS).
Multicast Group IP Address	Broadcast address used when communicating to all other multicast devices. This address will need to be the same on all communicating multicast devices.
Multicast Group Port	Multicast port used when communicating to all other multicast devices. This will need to be the same on all communicating multicast devices.

3.13 Digital Input/Output

The functionality of the shared digital input/output pin may be configured via the Transfer webpage. Because this pin is shared, the digital input status will be On when the digital output is set On.

The digital I/O channel can be transferred to/from another device using Modbus (see “3.14 Modbus I/O Transfer”) or it can be configured to provide status of the module communications. If the 945U-E disassociates from another

unit (that is, there is no wireless link), you can configure the digital output to turn On (set) or Off (drop).

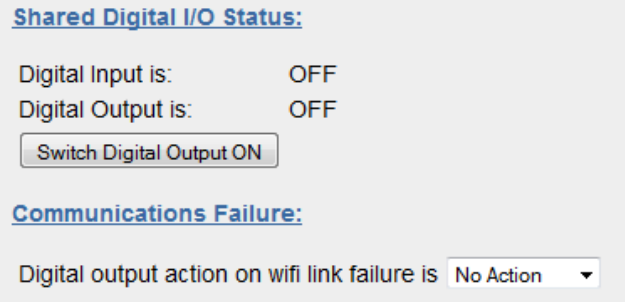


Figure 39 Digital I/O

3.14 Modbus I/O Transfer

The 945U-E provides Modbus TCP client and Modbus TCP server functionality for I/O transfer. The 5000 x 16-bit general purpose registers are provided for Modbus (including the onboard digital input/output) and are shared for both client and server. Modbus TCP client (master) and Modbus TCP server (slave) are both supported simultaneously, and when combined with the built-in Modbus TCP to RTU gateway, the 945U-E can transfer I/O to or from almost any combination of Modbus TCP or RTU devices.

The layout of the 945U-E I/O registers is summarized in the table below. Each register is internally saved as a 16 unsigned integer value. A Modbus transaction may access the entire 16-bit value of any register, or alternatively the most significant bit of a register may be accessed as a discrete value. The main use for the general purpose I/O registers is for intermediate storage, as when transferring I/O from one Modbus slave device to another. Also provided is the status of the onboard digital I/O, as well as the status of the wireless link and any serial or TCP connections.

An inverted status of registers 4300–4307 are also available and can be found at register locations 4370–4377.

The status register will contain the value FFFF (hexadecimal) for On and 0000 (hexadecimal) for Off.

Registers	Purpose
1–4299	General purpose I/O registers (read/write).
4300	On-board digital input value (read only).
4301	Link status (read only).
4302	Serial gateway connection status (RS232).
4303	Serial gateway connection status (RS485).
4304	TCP-RTU connection status (RS232).
4305	TCP-RTU connection status (RS485).
4306	TCP-RTU Modbus server connection status.
4307	Multicast pipe connection status.
4310	TCP-RTU number of connections (RS232).
4311	TCP-RTU number of connections (RS485).
4312	TCP-RTU Number of Connections (Modbus Server).
4320	On-board digital output value (read/write).
4370	On-board digital input inverted value (read only).
4371	Link status (read only) inverted.
4372	Serial gateway connection status (RS232) inverted.
4373	Serial gateway connection status (RS485) inverted.
4374	TCP-RTU connection status (RS232) inverted.
4375	TCP-RTU connection status (RS485) inverted.

Registers	Purpose
4376	TCP-RTU Modbus server connection status inverted.
4377	Multicast pipe connection status inverted.
4378–4999	Reserved for future use.

Modbus TCP client (master) enables the 945U-E to connect to one or more Modbus TCP servers (slaves). All Modbus master messages are directed to/from the onboard I/O registers, depending on configuration (described below). The Modbus TCP client may also poll Modbus RTU (serial) devices connected to either the local serial port or a remote 945U-E serial port by enabling the Modbus TCP to RTU gateway at the corresponding serial port (see “3.10 Serial Port Configuration”).

Modbus TCP client functionality allows a maximum of 100 mappings to be configured and a maximum of 25 different Modbus TCP servers. Modbus TCP server (slave) enables the 945U-E to accept connections from one or more Modbus TCP clients (masters).

All Modbus transactions routed to the onboard Modbus TCP server are directed to and from the onboard general purpose I/O registers. The Modbus TCP server is shared with the Modbus TCP to RTU gateway, so that the Modbus device ID is used to determine if a Modbus transaction is to be routed to the onboard Modbus TCP server or to a Modbus RTU device connected to the serial port. Care should be taken to ensure that all serially connected Modbus devices use a different Modbus device ID (Modbus slave address) than the onboard Modbus TCP server. Up to 32 separate connections to the Modbus TCP server are supported.

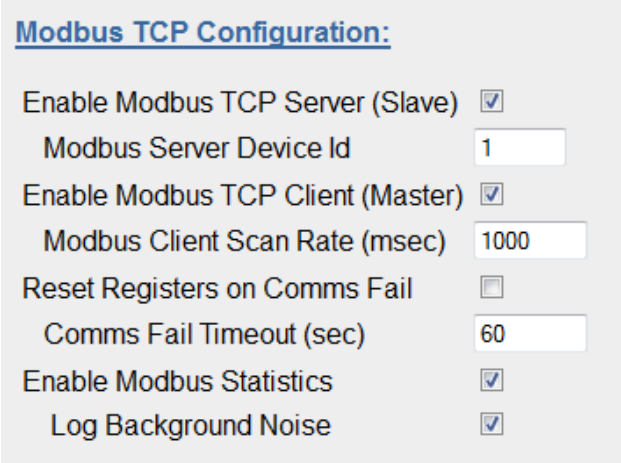


Figure 40 Modbus TCP

Modbus RTU (serial) master functionality is achieved by combining the Modbus TCP client (master) and Modbus TCP to RTU gateway. Simply specify a Modbus TCP client (master) connection to a Modbus TCP server, where the server is the address of any 945U-E with Modbus TCP to RTU gateway enabled. Care should be taken to ensure that the device ID (Modbus address) of the serial device is different to the device ID of the onboard Modbus TCP server of the 945U-E to which the serial device is connected.

The 945U-E provides a configurable option to automatically reset the value of the onboard I/O registers to zero in the event of a communications failure. If a valid Modbus transaction directed to and from a given register has not been completed for longer than a configurable timeout, the value of that register will be reset to zero.

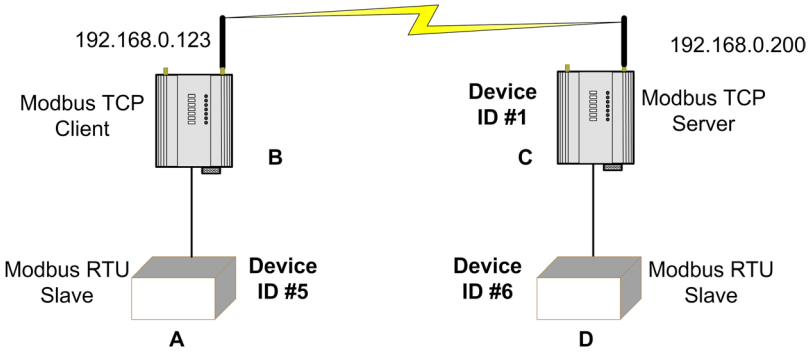


Figure 41 Modbus

An example of the Modbus functionality of the 945U-E is illustrated below. In this example, the status of the onboard digital input at C will be reflected at the onboard digital output at B. Also, 8 single-bit registers from Modbus serial device D will be transferred to A.

Modbus TCP Client Mappings:

Add Entry | Delete Entry

#	Local Register	IO Count	Function Code	Destination Register	Device Id	Server IP Address	Response Timeout (ms)	Comm Fail Register
1	4300	1	15: Write Coils	4320	1	192.168.0.200	1000	0
2	1	8	02: Read Discretes	1	6	192.168.0.200	1000	0
3	1	8	15: Write Coils	1	5	192.168.0.123	1000	0

Figure 42 Modbus Mappings for Unit B

Unit C is configured with Modbus TCP server enabled and device ID set to 1, so that the Modbus TCP client at unit B can connect and read the status of the onboard digital input. Unit C also has the Modbus TCP to RTU gateway enabled (see “RS-232 / RS485 Modbus TCP/RTU Converter” on page 43) so that the Modbus TCP client at unit B can communicate with the serial Modbus RTU device D.

Unit B is configured as shown above in Figure 42. The first mapping will write the register 4300 (local digital input) to server IP address 192.168.0.200 (Unit C), device ID #1 and register 4320 (digital output).

The second mapping shows a Modbus read command of 8 discretes, starting at register 1 (Destination Register) on device ID #6 connected to IP address 192.168.0.200, and storing the values locally at register #1 (itself).

The third mapping shows the Modbus write command (write coils), which is writing the local 8 I/Os starting at register 1 across to server IP address 192.168.0.123, device ID #5, destination reg #1.

Since the 945U-E supports Modbus TCP client and server simultaneously, the Modbus TCP server for unit B above could also be enabled. This would allow one (or more) external Modbus TCP clients anywhere on the extended wired or wireless network to connect to unit B and monitor the status of the I/O registers, including the I/O at units A, C, and D. This is a very powerful and flexible feature which could, for example, be exploited by a central monitoring facility or SCADA.

Modbus TCP Configuration on I/O Transfer Menu

Enable Modbus TCP Server (Slave) Select this checkbox to enable the onboard Modbus TCP server. All Modbus TCP connections to the module IP address and specified Modbus server device ID will be routed to the onboard I/O registers.

Modbus Server Device ID Specify the Modbus device ID for the onboard Modbus TCP server. Allowed values are 0 to 255.

Enable Modbus TCP Client (Master) Select this checkbox to enable the onboard Modbus TCP client. I/O to be transferred via the Modbus TCP client is specified with Modbus TCP client mappings.

Modbus Client Scan Rate	Enter the delay (in milliseconds) between execution of consecutive Modbus TCP client mappings to the same server.
Reset Registers on Comms Fail	When enabled, the value in any onboard I/O register will be reset to zero if a valid Modbus transaction directed to/from the given register has not been completed for longer than the Comms Fail Timeout.
Comms Fail Timeout	The period of time after which onboard I/O registers will be reset if a valid Modbus transaction directed at that register has not completed.
Enable Modbus Statistics	Enables the Modbus Diagnostic registers, as shown in "4.9 Internal Diagnostic Modbus Registers." Disabling this option will free up the registers and also slightly increase processing resources.
Log background Noise	RSSI & BGND on RX messages are made available in the diagnostic registers (see "4.9 Internal Diagnostic Modbus Registers" for details). For a hexadecimal value of 5F5D the 5D byte = RSSI and the 5F byte = BGND. Convert the value from hexadecimal to decimal and add a "-" (for example, 5F = -95dB). Disabling this option removes the background noise byte from these registers and therefore only the RSSI value is made available.

Modbus TCP Client Mappings on I/O Transfer Menu

Local Register	Enter the starting onboard I/O register number that the specified Modbus master transaction will transfer I/O to/from.
I/O Count	Specify the number of consecutive I/O register to be transferred for the specified transaction.
Function Code	Specify the Modbus function code for the transaction.
Destination Register	Enter the starting I/O register number in the destination device that the specified Modbus master transaction will transfer I/O to/from.
Device ID	Enter the Modbus device ID of the destination Modbus device.
Server IP Address	Specify the IP address of the destination Modbus TCP server for the specified transaction.
Response Timeout	Enter the timeout (in milliseconds) to wait for a response to the specified transaction.
Comm Fail Register	Enter the onboard I/O register number to store the communication status of the specified transaction. The specified register will be set to 0 if communications is successful, 0xFFFF if there is no connection to the specified server, or 0xFFxx where "xx" is the Modbus exception code

3.15 Roaming

In certain cases a client may be in a mobile situation and require a method of roaming to another access point. Normal network communications provide only basic roaming behavior, which means as the client moves further from the access point it will go through a period of poor communication followed by a complete disconnection of the radio link. It is at this point that the client will scan for access points, and if one is in range it could take up to 10 seconds for the client to establish a connection.

Fast roaming will significantly reduce the time taken for a client to roam from access point to access point. In addition, the discovery of access points is completed before the existing radio link deteriorates, therefore eliminating the periods of poor performance during transition to the next access point.

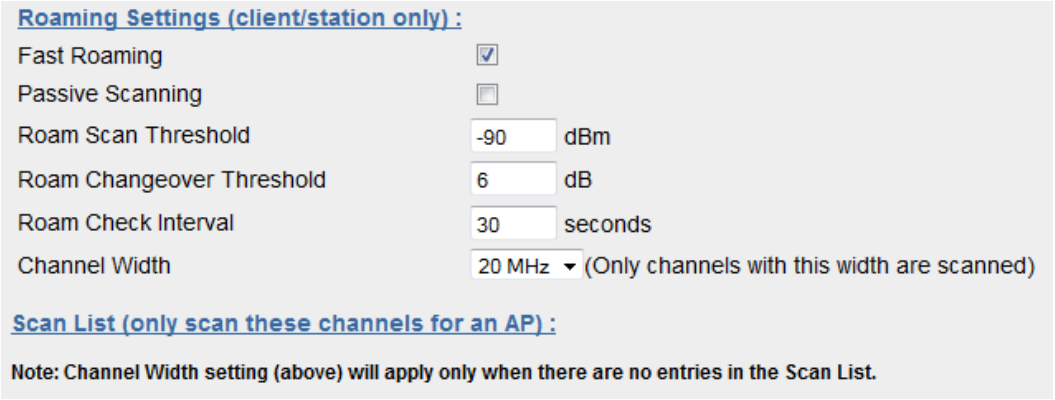


Figure 43 Roaming

The following settings and thresholds can be configured to fine tune the fast roaming process.

Fast Roaming	Fast roaming allows a client (station) to roam to an access point with a stronger signal strength without disrupting communications, or roam seamlessly between multiple access points based on configuration parameters, such as RSSI threshold.
Passive Scanning	(STA only.) Selecting this checkbox stops a client device from sending probe request messages when it is searching for an access point to connect to. Instead, the client waits for a beacon transmission from the access point. Passive scanning should be disabled when fast roaming is enabled.
Roam Scan Threshold	Background scan will be initiated when the RSSI to the currently connected AP drops below this threshold and fast roaming (above) is enabled. Default is -90 dBm.
Roam Changeover Threshold	This is the RSSI value above the roam scan threshold that is required for the client to change to the new access point. In the example shown above, the access point RSSI would need to be above -84 dB before it would change over. In general, the roam changeover threshold should be at least 6 dB, otherwise changeovers could occur too frequently.
Roam Check Interval	If a better access point is not found, the background scan is repeated every roam check interval, while the signal strength to the currently connected AP is below the roam scan threshold.
Channel Width	The channel width setting will apply only when there are no entries in the scan list. This allows you to select channel width bands for the background scan. If 5 MHz is selected, only 5-MHz channels will be scanned during the background scan. Default is Auto, which means all channels will be scanned.
Save Changes	Saves changes to non-volatile memory. Changes will not take effect until module is reset.
Save Changes and Reset	Saves changes to non-volatile memory and reset module.

When fast roaming is enabled, the client goes off-channel and periodically performs a background scan to identify available access points. When access points are identified, the RSSI is recorded as a potential connection. It takes 50 msec to scan each channel, with a 1-second delay between each scanned channel. Scanning 10 channels will take 10 seconds, during which time latency of up to 50 msec will occur and any throughput traffic is essentially paused and buffered for retransmission when complete. It is therefore recommended the scan list be used to limit the number of channels the client needs to scan, thus reducing the overall scan time.

During the background scan a client will scan all of the channels in the scan list to identify better access points. If no channels are configured, it will scan all channels.

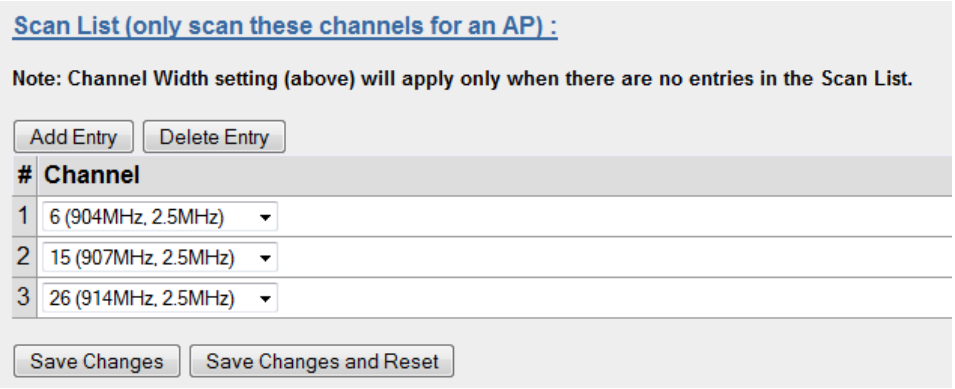


Figure 44 Scan List

The configuration in Figure 44 shows that the client will start scanning when the RSSI of its current connection to the access point falls below -90 dBm. When this happens it will scan the list of access points configured in the roaming scan list (in this case, channels 6, 15, 16 and 26), and if any of the RSSI levels are greater than -84 dBm, it will change to this access point, i.e. 6 dB (Roam Changeover Threshold) better than -90 dBm (Roam Scan Threshold).

3.16 Repeaters (WDS)

The range of a wireless network can be extended by allowing access points to behave as repeaters and forward traffic to other access points. Access point to access point communications is also known as wireless distribution system (WDS). The 945U-E offers very powerful WDS configuration, allowing for a mesh network with self-healing functionality. Alternatively, fixed access point to access point links can be configured for optimized throughput.

Each 945U-E access point supports up to 10 separate interfaces for WDS links to other devices. Each WDS interface can be either a bridge or router interface. Refer to “1.0 Network Topology” for more information on bridge versus router. If you need a simple repeater network (Figure 45), use a bridge interface.

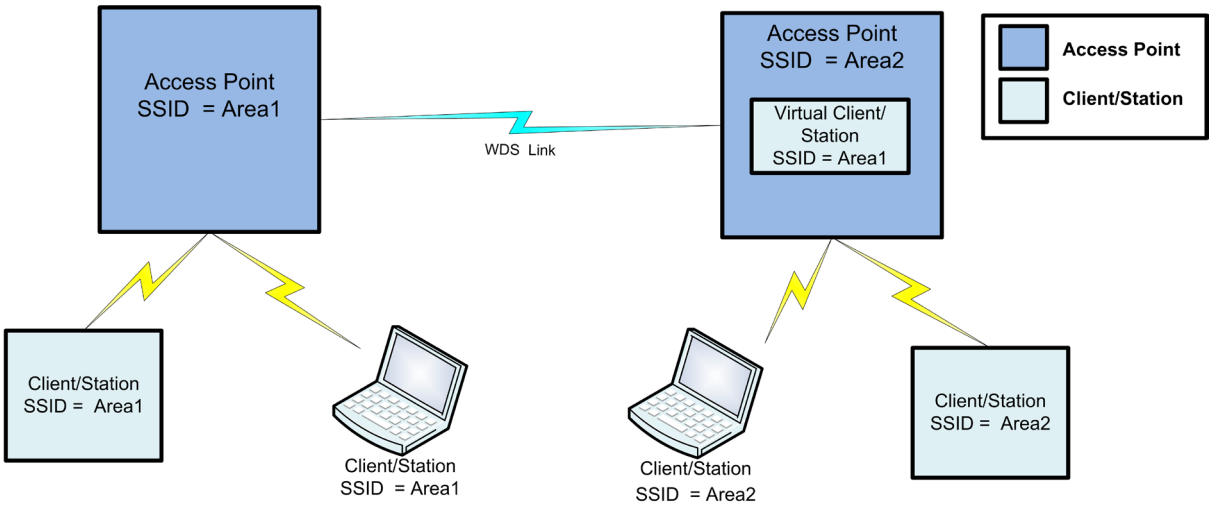


Figure 45 WDS Repeaters

A WDS bridge interface allows traffic to be bridged to another access point on the same IP network. WDS bridge interfaces do not require additional IP address configuration because they are bridged with the standard wireless interface that is used for connections to associated clients. All of the WDS interfaces on the one access point may be bridged, if required.

WDS bridge interfaces have the advantage that redundant paths are permitted when using the bridge Spanning Tree Protocol (see “3.5 Spanning Tree Algorithm”), thus behaving as a self-healing mesh network. Bridged networks are also not as configuration intensive as routed networks because WDS bridge interfaces generally do not require

IP address configuration (they inherit the IP address of the standard wireless interface).

A WDS router interface allows traffic to be routed to an access point on a different network, and therefore requires configuration of an IP address to reflect the network address of the destination network. WDS router interfaces cannot provide the redundancy of bridge interfaces, but can be used to reduce radio bandwidth requirements because the router can determine the destination based on IP address, whereas the bridge must go through a learning phase where all broadcast traffic must be retransmitted on each interface. Routed networks may also be used in some cases to avoid the overhead introduced by the bridge Spanning Tree Protocol when network loops exist.

Important Notes

- All access points must be configured on the same fixed radio channel. Auto Channel Selection must not be selected (see the Radio Configuration page for details on configuring the channel.)
- Specify SSID for AP/STA modes or MAC address for Point-to-Point mode.
- Router IP and Subnet fields should be left blank unless that WDS interface is to be on a different subnet. Leaving these fields blank will mean that the WDS interface will be bridged with the default wireless interface.
- Encryption is not inherited from the main page.
- Each WDS interface can also be configured with a different encryption algorithm. However, each side of a single WDS link must specify the same encryption algorithm and keys.
- When adding WDS router interfaces, you may need to add a routing rule on the Routing configuration page.
- When VLANs are enabled, router IP and subnet are ignored and the WDS interface is bridged depending on membership to a VLAN group.
- Spanning Tree Protocol (STP) column only applies when two or more interfaces are bridged.
- A maximum of 10 WDS connections can be configured. A combined maximum of five virtual access points and five virtual client/STA applies.
- WPA-Enterprise configuration is shared with the base access point (Authenticator) or station (Supplicant).

WDS connections are made by adding one or more virtual modules to an access point (see Figure 45). Each virtual module can be configured with one of the standard Wi-Fi operating modes (Access Point or Station) or a non-standard Point-to-Point mode.

- Access point and station virtual modules allow for the possibility of dynamically created connections (based on SSID) and support WPA encryption. A combined maximum of five access points and STA virtual modules can be configured per unit.
- Point-to-Point mode virtual modules provide static connections (based on MAC addresses), and cannot support WPA encryption. Point-to-point virtual modules should only be used for establishing WDS connections with third party access points that do not support standard WDS operation.

WDS Connections

The WDS Configuration page is accessible from the “Repeaters” link on any of the configuration webpages. The configurable WDS parameters are summarized below.

Add Entry Button	Add an entry to the WDS connections table. This adds a virtual station to the device.
Delete Entry Button	Delete the currently selected entry in the WDS connections table. To select (highlight) a row, click anywhere in the row.
Connection Mode	Specify the connection mode for this link. AP (Downlink) configures the connection as a virtual access point. Sta (Uplink) configures the connection as a virtual client. Point-to-point configures the connection as a fixed link.

SSID / MAC Address	AP Mode—Specify the SSID that this virtual access point will use. Stations connecting to this virtual access point use this SSID. Sta Mode—Specify the SSID that this virtual station will use when connecting to other access points. Point-to-Point Mode—Specify the MAC address of an access point with which a fixed link will be established. Usually only required for third-party devices.
Encryption	Select the required encryption (if any) for this WDS link.
Encryption Key	Enter the encryption key (for WEP encryption) or the passphrase (for WPA encryption). For WEP encryption, the encryption key is set as WEP Key 1. For Sta mode, this must match WEP Key 1 on the access point this virtual client will connect to. For AP mode, clients must configure their WEP Key 1 to the same value as this key and select the Default WEP Key to be WEP Key 1.
Router IP	Leave this field blank if this WDS interface is to be bridged with the default wireless interface. Otherwise, enter the IP address for this connection that specifies the IP network to which messages are routed.
Router Subnet	Leave this field blank if this WDS interface is to be bridged with the default wireless interface. Otherwise, enter the subnet mask of the network to which messages are routed.
STP	Applicable to WDS bridged connections only. Select the STP option if you wish to enable the bridge Spanning Tree Protocol on this connection.

There are many ways to setup wireless networks. Often it depends on the devices you wish to connect and the existing network topology. The following pages show some examples of how to connect devices into different types of systems.

Example 1: Extending Range Using WDS

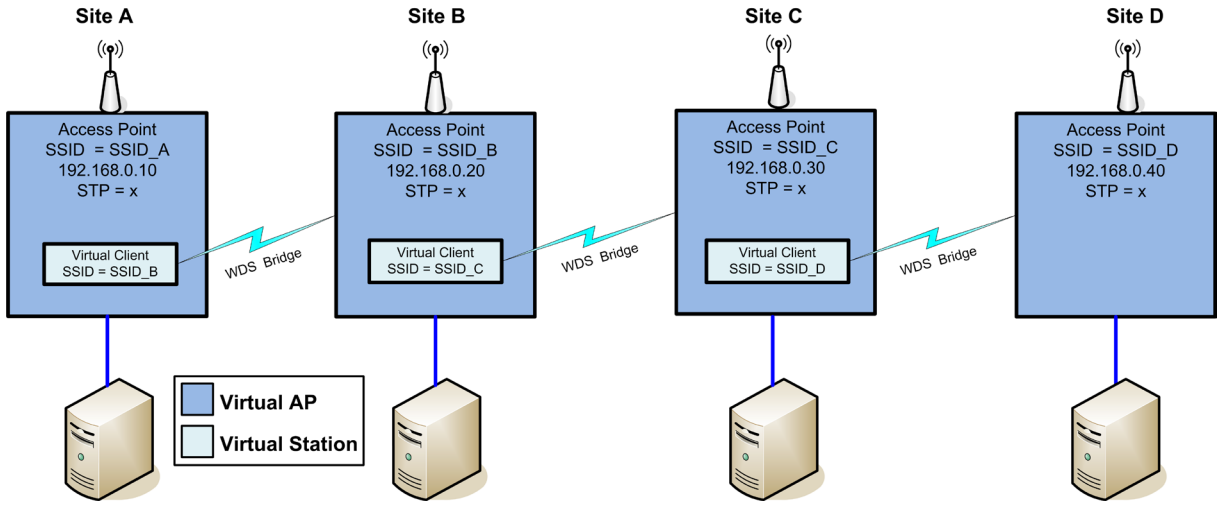


Figure 46 Extending Range

One of the most common uses for WDS is to extend the range of the wireless network using repeaters. Figure 46 illustrates a simple example where the four access points are all at fixed locations (each of the access points could, have one or more client/stations connected). Since the locations are fixed, you can avoid the overhead of using the Bridge Spanning Tree Protocol by configuring fixed WDS links to ensure that each access point will only connect to the next access point in the chain. Any number of additional intermediate repeaters could be added to the chain in a similar way.

WDS Connections:

Add Entry | Delete Entry

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Client / Station (Uplink)	SSID_C	WPA2-PSK(AES)	PassPhrase			☑

Figure 47 Site B WDS Configuration 1

The WDS configuration for unit B is shown above (this page is accessible via the Repeaters link from the configuration webpages). Site B is acting as an access point for Site A, and is a client to Site C, likewise Site C is acting as an access point for Site B, and a client for Site D. Since this example is a bridged network (all devices are on the same IP network and each link is using a different SSID), there is no possibility of loops (multiple paths to the same location), and therefore we do not need to incur the overhead of enabling STP (bridge Spanning Tree Protocol).

We specify the devices at the other end of the WDS links by SSID only. MAC addresses can be used to specify point-to-point links to third party devices which do not support meshing via SSID.

In this example, each virtual connection is using the same encryption method (WPA-PSK (AES) with a key of “Pass Phrase.” However, in Example #1 the Encryption method and key can be different for each virtual link or even disabled (no encryption). Also the Spanning Tree Protocol is disabled as there is no possibility of network loops.

Example 2: Roaming with WDS Access Points

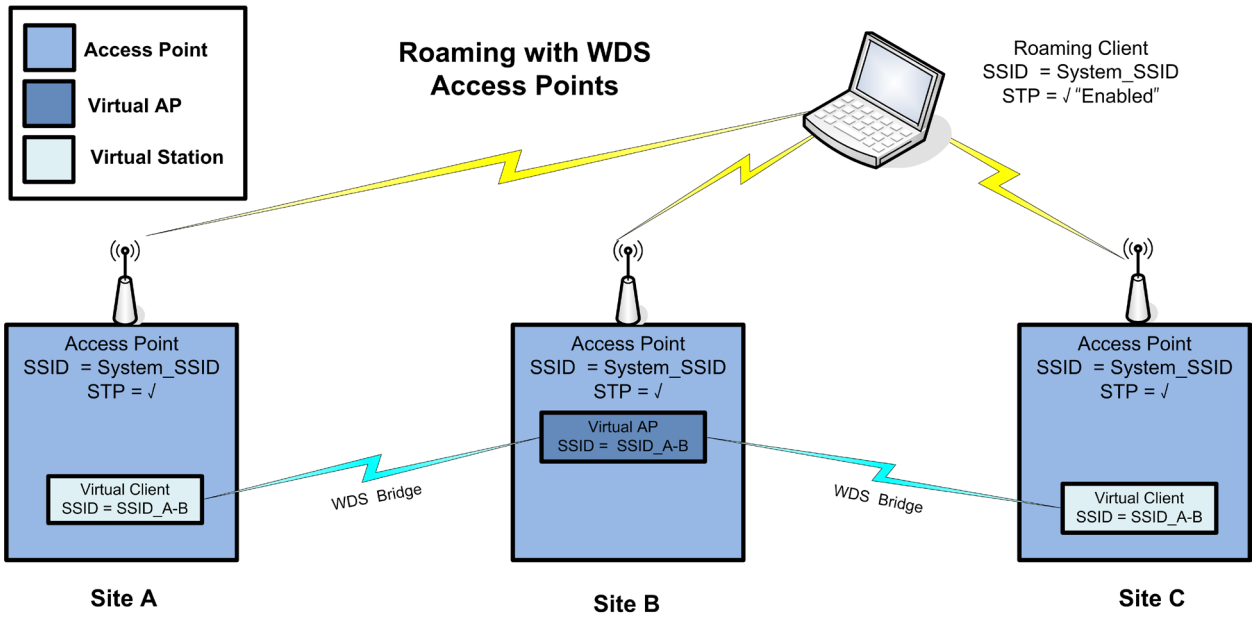


Figure 48 WDS Roaming

Another common use for WDS is extending the range across a large wireless network by allowing roaming connections between access points or being able to switch to the next access point when out of range of the previous access point. Figure 48 shows a bridging network with a number of access points all with the same SSID and network structure, so the Stations can freely roam between access points.

Each access point then needs a separate connection to the next access point, which is provided using the WDS Virtual Access Points and Stations. Site B is acting as a virtual AP for Site A, which in turn is acting as a virtual station. At the same time Site B is also acting as a virtual station for Site C which in turn is acting as a virtual access point. This setup can be replicated to extend the range and will allow any roaming stations full connectivity across the network.

WDS Connections:

Add Entry | Delete Entry

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Access Point (Downlink)	SSID_A-B	WPA2-PSK(AES)	PassPhrase			☑

Figure 49 Site B WDS Configuration 2

Example 3: Adding Redundancy

In the example below, 4 x access points (A, B, C, & D) form a mesh network using only WDS bridge interfaces. Each of the access points may also have its own associated clients. Each access point is configured with a different SSID, which means that the clients associated with each access point are fixed.

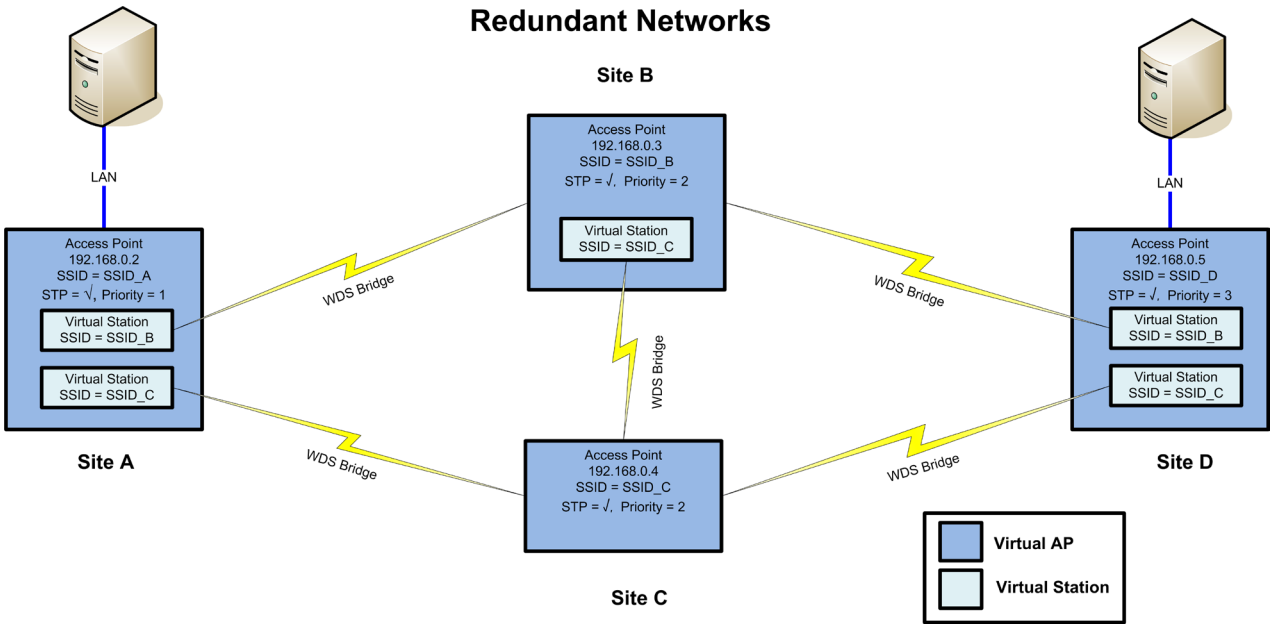


Figure 50 WDS Redundancy

Sites A, B, C, and D can all exchange data with each other (as can all of their stations) as if they were all on the same wired segment. Notice that there are redundant paths, and therefore the possibility for loops to occur.The bridge Spanning Tree Protocol should therefore be enabled, and depending on the size of the mesh, a bridge priority should possibly be configured.

Bridge priority is used to determine the connection priority when selecting an interface to put into the forwarding state. You can assign higher priority values to interfaces that you want spanning tree to select first, and lower priority values to interfaces that you want spanning tree to select last. If all interfaces have the same priority value, the MAC address is used to work out the priority.

To illustrate the redundancy, consider that if Site A needs to send data to Site D it has redundant paths through both B and C. However, due to the Spanning Tree Protocol only one of B or C will relay the data, with the other taking over in the event of a failure.

In this example, Site B uses its primary access point to act as an access point for virtual stations on Site A and D, and uses a virtual station to act as a client to Site C. Sites A & D use two virtual stations to act as clients to Site B and to Site C. The configuration for Site B and A & D are shown below.

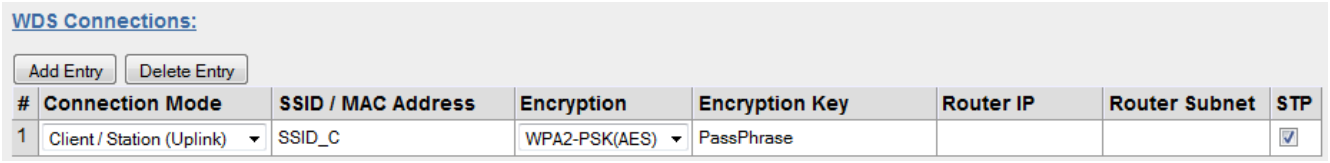


Figure 51 Site B WDS Configuration

Figure 52 Site A and D WDS Configuration

Encryption levels and key above are shows as being different, but they can be the same as in some of the earlier examples. One reason why the encryption level and key would be different is that the access point may have clients that communicate using a different encryption method (for example, 128-bit WEP) and may not support the same encryption method.

Example 4: WDS Routed Network

An example of using WDS router interfaces to achieve a similar physical topology to the WDS bridge example discussed earlier is shown in Figure 53.

In both examples, there are four WDS access points each with the possibility of having their own client or stations associated. In both examples, Sites A, B, C, and D can all exchange data with each other. The bridged example has the advantage of redundancy, but at the expense of extra overhead. The routed example below cannot provide the redundancy of the bridged example, and requires more configuration effort, but does not have the overhead of using the bridge Spanning Tree Protocol and therefore is suited to fixed installations that do not require redundancy.

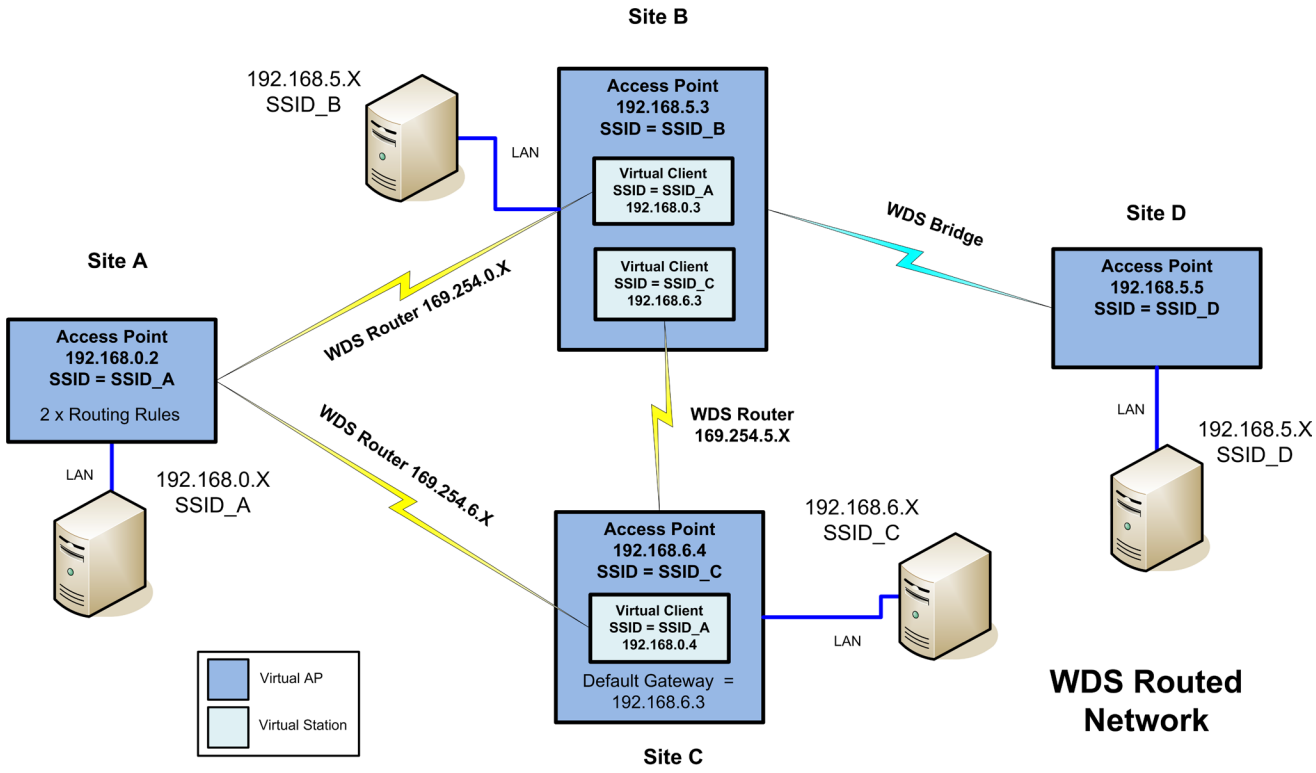


Figure 53 WDS Routed

Each modem has a different SSID. This is done to limit broadcast traffic and to route data only were it needs to go. Site B has two virtual client WDS links configured—one to Site A's access point, and one to Site C's access point. Figure 54 shows the WDS connections at Site B.

WDS Connections:

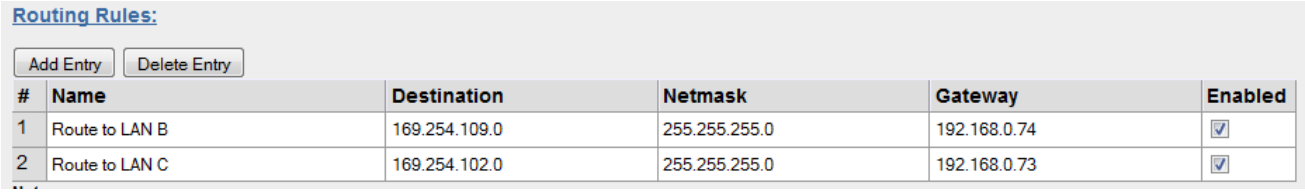
Add Entry | Delete Entry

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Client / Station (Uplink)	SSID_A	WPA2-PSK(AES)	PassPhrase1	192.168.0.3	255.255.255.0	☐
2	Client / Station (Uplink)	SSID_C	WPA2-PSK(AES)	PassPhrase2	192.168.6.3	255.255.255.0	☐

Figure 54 Site B Configuration

- The first entry configures a virtual WDS client connection from Site B to the access point at Site A. The SSID is the same as Site A and the router IP address is 192.168.0.3, which is on the same subnet. Encryption is not inherited from the main page. Therefore, if the encryption method/key are left blank the WDS link will be open. This example shows the encryption method and keys as being different, but they can be the same or take on the same method and key as the main wireless interface.
- The second entry configures another virtual WDS client connection but this time to the access point of Site C. Again, the SSID is the same as the access point, and the router IP is on the same subnet as the access point

In addition to adding these WDS connections, Sites C and D will need a default gateway address configured so that the modules can determine where to send traffic destined for the other networks. In addition, because Site A does not know how to get to networks 192.168.5.0 and 192.168.6.0, it requires rules to confirm the routing paths. A default gateway and one routing rule could be configured, but it is easier to configure two routing rules, as shown in the example in Figure 55.



Routing Rules:

Add Entry | Delete Entry

#	Name	Destination	Netmask	Gateway	Enabled
1	Route to LAN B	169.254.109.0	255.255.255.0	192.168.0.74	☑
2	Route to LAN C	169.254.102.0	255.255.255.0	192.168.0.73	☑

Figure 55 Site A Routing Rules

- The first routing rule specifies 192.168.5.0 as the destination with a netmask of 255.255.255.0 (network address range of Site B). Because the last byte of the destination IP is zero, this refers to the network (192.168.5.1 – 192.168.5.254) as opposed to an individual host IP. The same rule specifies the address 192.168.0.3 as the gateway address. The routing rule effectively tells the 945U-E that any traffic destined for network 192.168.5.X should be forwarded to Site B via WDS link address 192.168.0.3.
- The second routing rule is similar, except the destinations IP address range is 192.168.6.0 with a netmask of 255.255.255.0, indicating all traffic for the 192.168.6.X network will be routed through the WDS link address 192.168.0.4. This is the WDS router IP address that Site C has been configured with for its WDS link to Site A.

For more information on routing rules, refer to the “3.17 Routing Rules.”

Unit C and D require some sort of routing rule that will determine how they communicates to networks outside of their configuration. Similar routing rules as shown above could be configured to direct traffic to these other networks, but if only one routing path is required a default gateway address can be configured on the Network page.

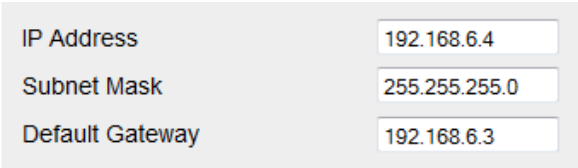


Figure 56 Gateway Address

3.17 Routing Rules

When a 945U-E receives an IP frame that is destined for an IP address on a different network, it checks if the network address matches the network address of one of its own interfaces (hard-wired Ethernet, wireless Ethernet, or WDS) and forwards the frame appropriately. However, if the IP network address does not match the network address of any of its interfaces, the 945U-E will forward the frame to its default gateway. In this case, it is assumed that the default gateway has a valid route to the destination.

In some cases, it is not practical to have just one default gateway. For example, this is true for routed wireless networks with more than two 945U-E routers, and in some cases when WDS router interfaces are used. If more than one next-hop router is required, the 945U-E allows for up to 30 routing rules to be configured. A routing rule specifies a destination network (or host) IP address and the corresponding next-hop router that messages for the specified destination will be forwarded to. It is assumed that the next-hop router (or gateway) will then deliver the data to the required destination (or forward it on to another router that will).

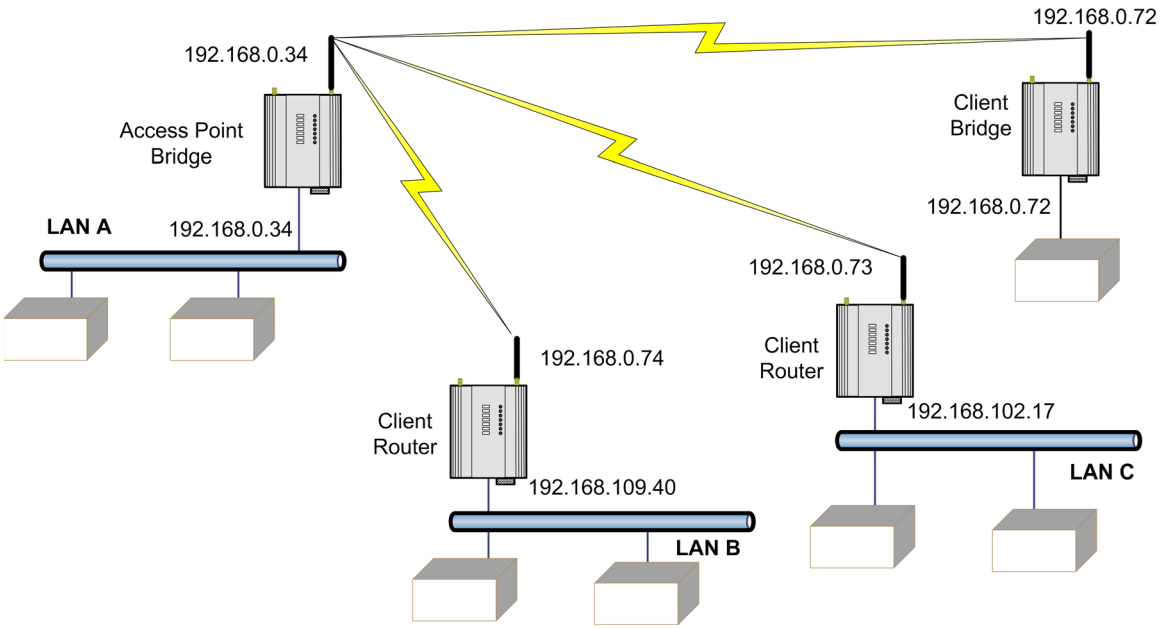


Figure 57 Routing

Figure 57 illustrates a situation where routing rules may need to be configured. In this example, the 945U-E clients need only specify the access point as their default gateway (they require no routing rules to be configured). However, for the access point to be able to deliver traffic to LAN B and LAN C it needs to have routing rules configured that specify the respective 945U-E client/routers as next-hop routers (gateways) to networks B and C. Note that devices on LAN A should specify the 945U-E access point as their default gateway. An alternative to adding routing rules to the 945U-E in this example would be for each device on LAN A that needs to communicate with LANs B and C to have independent routing rules specifying the 945U-E clients at B and C as gateways to those networks.

The routing rules for the access point in the above example are shown below. The first entry shows the route to LAN B. The gateway for the route to LAN B is configured as the wireless IP address of the 945U-E client connected to LAN B. The destination for the route is configured as the network address of LAN B. Because the host ID of the destination IP address is 0, it specifies a network address. Consequently, any traffic received at the access point with destination IP address 169.254.109.x (where “x” is any host ID) will be forwarded to the 945U-E at LAN B.

Devices on LAN B and LAN C that need to send messages back to LAN A will need to have their gateway addresses directed to the 945U-E on their respected networks (for example, a LAN B device needs to send data back to LAN A). The gateway address will need to be configured as 169.254.109.40, because this is the IP address of the wired side of the LAN B 945U-E. Any message coming in with a 192.168.0.X IP address will be directed across the wireless interface to LAN A.

The Routing Rules configuration page can be accessed by selecting the “Routing” link on any of the configuration webpages. Up to 30 routing rules may be added to each 945U-E. The table below summarizes the configurable parameters of a routing rule.

Routing Rules:

Add Entry | Delete Entry

#	Name	Destination	Netmask	Gateway	Enabled
1	Route to LAN B	169.254.109.0	255.255.255.0	192.168.0.74	☑
2	Route to LAN C	169.254.102.0	255.255.255.0	192.168.0.73	☑

Figure 58 Routing Rules

Name	A name to describe the routing rule (maximum 32 characters).
Destination	The destination network (or host) IP address. To specify a network address, set the host address to 0. For example, an IP address 192.168.0.0 with netmask 255.255.255.0 would specify a destination network, while 192.168.0.16 specifies a destination host.
Subnet Mask	The subnet mask for the destination network.
Gateway	The IP address of the next-hop router for the specified destination.
Enabled	Select this checkbox to enable the rule. You can clear the checkbox to disable a routing rule without needing to re-enter the information at a later time.

NOTE Entering dedicated Ethernet Routes can also be added to the wired Ethernet LAN in place of generating or adding routing rules into the modems.

3.18 Filtering

When configured as a bridge, the 945U-E will transmit all broadcast messages appearing at its wired Ethernet port. When the 945U-E is configured as a router, this does not occur. In many cases, the intended recipient of the broadcast traffic does not lie at the opposite end of a proposed radio link. Reducing unnecessary broadcast traffic sent over the radio link will increase available bandwidth for data. The 945U-E has a filtering feature to help reduce unnecessary wireless transmissions and enhance security.

The 945U-E may be configured to reject or accept messages to and from certain addresses. To accept wireless messages from particular devices a “whitelist” of addresses must be made. Alternatively, to reject messages from particular devices, a “blacklist” of addresses must be made. Filtering applies only to messages appearing at the wired Ethernet port of the configured 945U-E.

The filter comprises of three lists—MAC addresses, IP address/protocol/port, and ARP filters. Each list may be set as either a blacklist (to block traffic for listed devices and protocols), or as a whitelist (to allow traffic for listed devices and protocols).

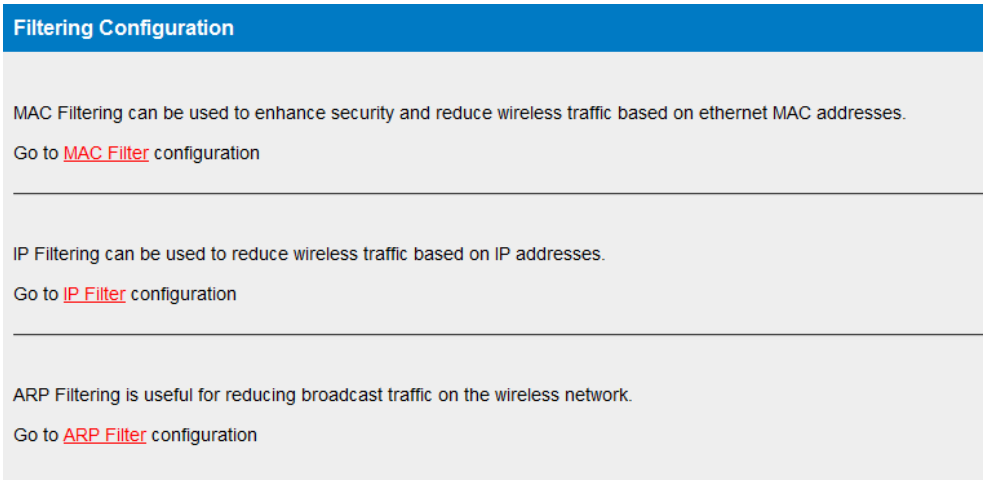


Figure 59 Filtering

The filter operates on the following rules:

- The MAC address filter is always checked before the IP address filter.
- If a message matches a MAC filter entry, it will not be subsequently processed by the IP filter. If the MAC filter list is a whitelist, the message will be accepted. If the MAC filter list is a blacklist, the message will be dropped.
- The MAC address list checks the source address of the message only.

- The IP address filter checks both the source address and the destination address of the message. If either address match, then the rule is activated.
- ARP filtering applies only to ARP request packets (typically these are broadcast packets) sourced from the Ethernet interface and destined for the wireless interface. ARP requests from devices on the wireless network will always be passed to the Ethernet interface. ARP response packets will always be passed.

When configuring a whitelist, it is important to add the addresses of all devices connected to the 945U-E wired Ethernet port that communicate over the wireless link. It is particularly important to add the address of the configuration PC to the whitelist. Failure to add this address will prevent the configuration PC from making any further changes to configuration. Design of the filter may be simplified by monitoring network traffic and forming a profile of traffic on the wired network. Network analysis software, such as the freely available “Wireshark” program, will list broadcast traffic sent on the network.

In the example in Figure 60, device B needs to communicate with device E via modems C and D. The filtering requires that at modem C has device B in its whitelist and modem D has device E in its whitelist. With this filtering, device A will be not be able to access device E, because device A is not present in the whitelist in modem C.

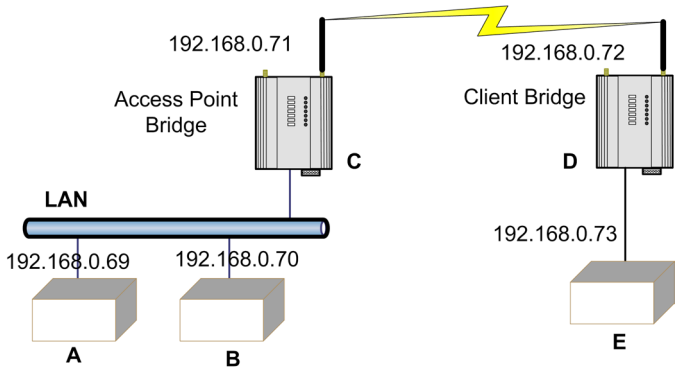


Figure 60 Filtering Example

NOTE If an erroneous configuration has prevented all access to the module, SETUP mode may be used to restore operation.

MAC Address Filter Configuration

MAC addresses are uniquely assigned to each device and therefore can be used to permit or deny network access to specific devices through the use of blacklists and whitelists. In theory, MAC filtering allows a administrators to permit or deny network access to hosts associated with the MAC address, though in practice there are methods to circumvent this form of access control through address modification. The MAC filter entry will match only the source MAC address in the packet.

NOTE It is important to add the MAC address of the configuration PC when creating a whitelist. If the configuration PC is not on the whitelist, it will be unable to communicate with the module for further configuration.

Select “Blacklist” or “Whitelist”	Blacklist will prevent all listed devices from accessing the module and using the radio link. Whitelist will allow devices with the MAC addresses listed to communicate with the module and utilize the radio link. All other devices are blocked.
Add Entry	Add a row to the table of Mac address filter rules.
Delete Entry	Delete the currently selected MAC address filter rule.
Enable	Select checkbox to enable the rule.
Mac Address	Enter the desired source MAC address.

Save Changes	Saves changes to non-volatile memory (reset is required to activate).
Save Changes and Reset	Saves to non-volatile memory and restart to activate changes.

IP Address Filter Configuration

The IP filter can be used to permit or deny network access to specific devices through the use of blacklists (blocking of traffic that matches a rule) and whitelists (allowing traffic that matches a rule). The IP filter entry will match either source or destination address in the packet. That is, if either the source or destination IP address falls within the address range specified in the rule, the packet is matched and will be discarded (blacklist) or allowed (whitelist).

If the protocol is specified, the protocol of the packet must also match. If the protocol is TCP or UDP, the source or destination TCP/UDP can also be inspected. If the IP address and protocol matches and the source or destination port number falls within the range specified, the packet is matched.

NOTE Configuration pages use TCP protocol on ports 80 and 443. Create whitelist rules specifying the configuration PC's IP address, with TCP protocol, ports 80 and 443.

Select "Blacklist" or "Whitelist"	Blacklist will prevent all listed devices from accessing the module and using the radio link. Whitelist will allow devices with the IP addresses listed to communicate with the module and utilize the radio link. All other devices are blocked.
Add Entry	Adds a row to the table of IP Address filter rules.
Delete Entry	Deletes the currently selected IP address filter rule.
Enable	Select this checkbox to enable the rule.
IP Address Min **IP Address Max**	These fields set the range of IP addresses. All addresses within the specified range are affected by the rule.
Port Min **Port Max**	When the protocol is set to TCP or UDP, this is the range of port addresses to which the rule applies. When protocol is set to All or ICMP, these settings have no effect.
Protocol	This chooses the protocol to which the rule applies. The rule can apply to Any protocol (All), or to only one of TCP, UDP, or ICMP (Ping).
Save Changes	Saves changes to non-volatile memory (reset is required to activate).
Save Changes and Reset	Saves to non-volatile memory and restart to activate changes.

ARP Filter Configuration

Address Resolution Protocol (ARP) is a broadcast message and is primarily used for finding a MAC address when only its IP or some other Network Layer address is known. On large networks, you tend to get a high proportion of broadcast messages. Using ARP filters is useful for reducing broadcast traffic on the wireless network by only allowing ARP requests for known units to pass, or by blocking ARP requests for high use addresses.

Select "Blacklist" or "Whitelist"	A blacklist will block ARP requests that match the entry. A whitelist will allow only ARP requests that match the entry. All other devices are blocked.
Add Entry	Adds a row to the table of ARP address filter rules.

Delete Entry	Deletes the currently selected ARP address filter rule.
Enable	Select this checkbox to enable the rule.
IP Address	This sets the IP address that you wish to filter.
IP Netmask	Sets the IP Netmask.
Save Changes	Saves changes to non-volatile memory (reset is required to activate).
Save Changes and Reset	Saves to non-volatile memory and restart to activate changes.

3.19 DHCP Client Configuration

DHCP (Dynamic Host Configuration Protocol) allows DHCP clients to automatically obtain their IP address at startup. This simplifies network administration because there is no need to manually configure each device with a separate IP address. The 945U-E is able to act as a DHCP client. To set the 945U-E to acquire its IP address from a DHCP server, select the checkbox “Obtain IP Address Automatically” on the Network Configuration page. When configured as a DHCP client, the “Device Name” on the Module Information page will be the module identifier (as the IP address will be unknown), and so should be given a unique name.

3.20 DHCP Server Configuration

The 945U-E is able to act as a DHCP server, supplying IP addresses automatically to other DHCP client devices. Note that the 945U-E units need to act in conjunction with their connected devices. If a connected device is a DHCP server, the local and remote 945U-E units can be configured as DHCP clients and receive IP addresses from the server device. Similarly, if a 945U-E is configured as a DHCP server it can provide IP addresses to DHCP clients—both 945U-E units as well as other connected devices. Configuration items for the DHCP server are listed below.

Enabled	Select this checkbox to enable the DHCP server.
IP Range Minimum / Maximum	The DHCP server will assign IP addresses to DHCP clients from within this range of addresses.
Gateway **Primary DNS** **Secondary DNS**	These settings are common to all of the DHCP clients, and refer to the gateway address, and Domain Name Service (DNS) configuration.
Lease Time	This is the number of seconds the client is granted the assigned IP address. The client should renew its lease within this time.

3.21 DNS Server Configuration

DNS (Domain Name Service) allows devices to be given human-readable names in additions to their IP address. This makes identification of devices (hosts) simpler, and makes it possible to identify devices that have been automatically assigned their IP address by a DHCP server (see “3.20 DHCP Server Configuration”). DNS is the system that translates Internet names (such as www.eaton.com/wireless) to IP addresses. The ELPRO 945U-E can act as a DNS server for a local network. Name to IP address mapping is automatically updated by the built in DHCP server when it issues an IP address to a client unit.

For the DNS server configuration to be effective, each DNS client must be configured with the address of this DNS server, as either the primary or secondary DNS (secondary DNS is only used if there is no response from the primary DNS). Normally this is done by setting the primary DNS field of the DHCP server configuration to the wireless IP address. This address is then provided to client units to use as their primary DNS server address when the DHCP server issues an IP address. The DNS server is configured using the following settings.

Enabled	Select this checkbox to enable the DNS server.

Domain Name	This is a common suffix applied to the name of each device in the network. If your network is part of a larger network, this would be assigned to you by the relevant naming authority. If your network is stand-alone, this field is set to an arbitrary name of your choice.
Device Name (Host Name)	This is the DNS name of the local device (commonly referred to as the host name or computer name). This setting is duplicated on the main Module Information configuration page. This is the name that is used to refer to this device (see “3.23 Module Information Configuration”).

3.22 VLAN

What is VLAN

VLAN (virtual local area network) is a way of splitting a network into groups that could extend beyond a single traditional LAN to groups of LANs, each identified with a different VLAN ID (VID). Using a VLAN, you can group users by logical connections instead of physical location. This can increase security and help improve the efficiency of traffic flow by limiting multicast and broadcast messages. Traffic between VLANs is blocked unless the VLAN is identified with the correct VLAN ID.

There are three main VLAN modes that the 945U-E supports:

- **VLAN (Pass-through Mode)**—A transparent bridge in which frames are forwarded unmodified. This is the default mode of the modem in which all frames pass transparently through the bridge regardless of whether they are VLAN tagged or untagged. This is the most common VLAN mode and requires no VLAN configuration at all. In VLAN Pass-through mode, access to the internal management functions is via untagged frames only, using the IP address and subnet mask configured on the Network page.
- **VLAN Aware (Bridging Mode)**—A VLAN bridge that allows only explicitly configured VLANs that correspond to the configured VLAN groups to pass data. VLAN Bridging mode is used when the tagging method is changed in a bridged network, for example, if a frame traverses from a VLAN group to an interface that is not configured in a VLAN. When a VLAN packet is passed to an untagged VLAN interface, the tag is removed so that the packet can properly enter the network. Similarly, if an untagged VLAN packet is passed to a VLAN group a VLAN tag is added. When one or more VLAN groups have been configured, VLAN Pass-through is disabled and VLAN Aware mode is enabled.
- **VLAN Aware (Routing Mode)**—Same as “VLAN Aware (Bridging Mode)” above, except that the VLANs are routed, not bridged. When a packet is routed from one VLAN to another on a different interface. The interfaces can be tagged or untagged, and are generally on different subnets.

Enabling VLANs will allow the module to facilitate a number of possible VLAN topologies, such as:

- Segregating a wireless network into multiple virtual networks.
- Functioning as the wireless backbone on a VLAN trunk.
- Enabling a wireless network or part of the wireless network to form a VLAN trunk.
- Defining multiple virtual networks, each with a different priority to define traffic class based forwarding behavior over the radio channel.

Each module can be set up to accept different networks by configuring VLAN groups and having the interfaces (such as Ethernet, wireless, or WDS repeater) configured to accept or reject tagged or untagged communications frames.

Operation

VLAN Pass-through is enabled by default in the modem. No VLAN configuration is needed, and modem will pass any VLAN tagged frames. To initiate VLAN bridge or router operation, VLAN Aware mode must be enabled on the VLAN page.

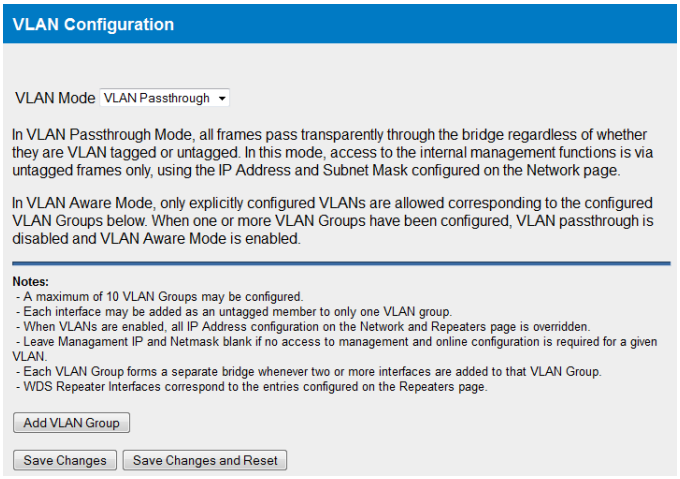


Figure 61 VLAN Pass Through

When VLAN is enabled a default “Management VLAN Group” is created, bridging the Ethernet and wireless interfaces and configuring both with untagged frames. The “Management IP” and “Management Netmask” addresses will override the modules “IP Address” and “Subnet Mask” and the Device Mode will be changed to “VLAN Bridge.” These changes will be indicated on the Network page of the module. A Management VLAN is created to ensure that the module will be accessible for configuration and diagnostics after setup.

If more than one interface is added to a VLAN group, a separate bridge will be created for the VLAN group. The configured interfaces for the VLAN group will then be configured as ports on the bridge.

In Figure 62, the Management VLAN has two interfaces configured, Ethernet and wireless, and both are set to “Untagged.” This means the module can be accessed by either Ethernet or wireless networks using untagged frames.

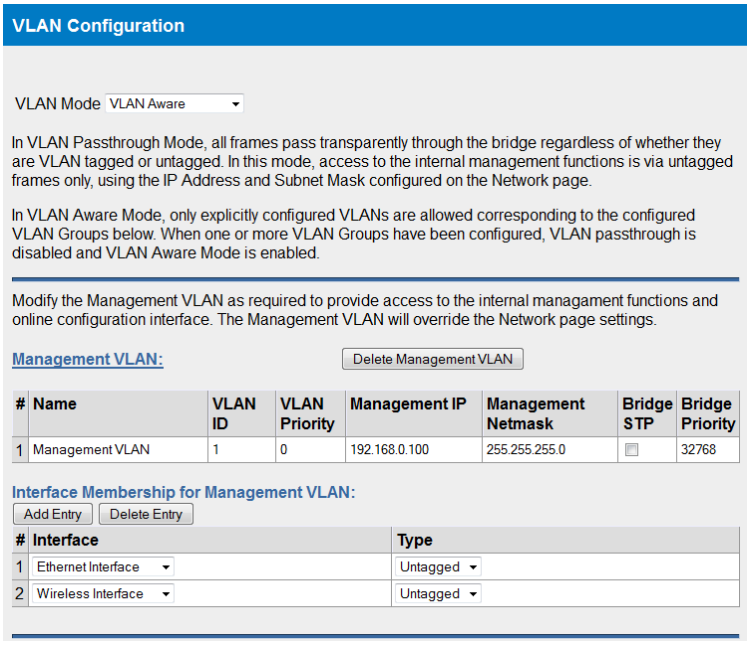


Figure 62 VLAN Aware

NOTE Leaving the default Management VLAN is advised, as it will ensure that the module is accessible through any interface.

VLAN Group

Enabling VLAN on the module will require one or more configurable VLAN groups. A maximum of up to 10 VLAN groups can be supported. Each VLAN group will contain the following configurable parameters and associated functionality.

Name — A textual description of the VLAN group, consisting of a maximum of 32 ASCII characters. This parameter is descriptive only and serves no functional purpose.

VLAN ID — A valid 12-bit IEEE802.1Q VID, with a range of 1–4095. The VLAN ID will be added to all outgoing VLAN tagged frames for this VLAN group. All incoming VLAN tagged frames for the VLAN group must have this VLAN ID.

VLAN Priority — An IEEE802.1Q-compatible, 3-bit Priority Code Point, with a range of 0–7, where seven is the highest priority, one is the lowest, and zero is the default, which is a mid-range "best-effort" value. The VLAN priority will be added to all outgoing VLAN tagged frames for this VLAN group. Furthermore, the VLAN priority will be used to determine which of 4 priority radio queues VLAN tagged frames will be queued on when transmitted via the radio.

Management IP — The management IP is the address of the module if only one VLAN group is configured. Access to the module's internal Web based configuration and IP-based functions (such as serial gateway, Modbus server) is provided via this management IP address and subnet mask.

NOTE If only one VLAN group is configured, it must have a management IP and netmask. If further VLAN groups are configured (groups 2–9), they only need a Management IP and subnet if access to the modules IP-based functions (such as Modbus or webpages) is required.

Management Netmask — The IP network mask of the Management IP (see above).

Bridge STP — Turns on Spanning Tree Protocol (STP) for the bridge. STP prevents network loops that can cause broadcast storms.

Bridge Priority — The STP priority number for the bridge. This value should be set in context with other devices that are connected on the same network.

Interface Membership

Each VLAN group has a configurable interface membership list. The membership list will allow up to twelve possible interfaces to be added. The following configurable parameters will apply to each entry.

Interface — Select an interface from the drop down list to be used for the VLAN group. Available interfaces are, Ethernet, Wireless, or one of the 10 WDS Repeater connections that correspond to configured entries on the Repeaters page.

Type — Specifies whether the interface is to support VLAN tagged or untagged frames. When untagged is specified, all incoming frames on the interface must be untagged, and all outgoing frames will be sent untagged. When tagged is specified, all incoming frames must have a VLAN tag with VLAN ID matching the configured VLAN ID for the VLAN group, and all outgoing frames on this interface will have a VLAN tag added with the configured VLAN ID and priority for that VLAN group.

Examples

Example 1: Basic VLAN

A common use for VLAN functionality in a module is to tag data from a VLAN-unaware device and send this to a VLAN trunk. A simple example of this involves bridging between Ethernet and wireless ports for just one VLAN. In the example illustrated below, the Ethernet interface is tagged and the wireless interface is untagged. Any data

arriving at the Ethernet port is expected to have VLAN tagged data with “VLAN ID 10” and any data sent from the Ethernet port will have the VLAN tag added. This example allows wireless data from VLAN-unaware devices to be bridged with the Ethernet interface and have VLAN tags added (the Ethernet connection is now part of a VLAN trunk that will send/receive data to/from other VLAN-aware devices).

Example 1

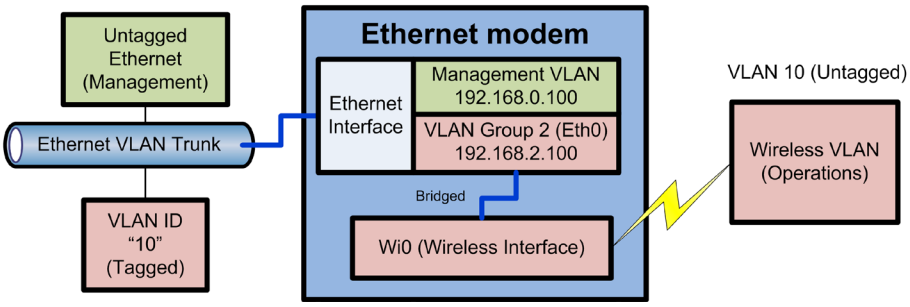


Figure 63 VLAN Example 1

The module configuration below shows there are two VLAN groups configured. The first group is used for management of the module and ensures a connection is maintained for configuration and diagnostics from untagged devices on the VLAN trunk.

Modify the Management VLAN as required to provide access to the internal managament functions and online configuration interface. The Management VLAN will override the Network page settings.

Management VLAN: Delete Management VLAN

#	Name	VLAN ID	VLAN Priority	Management IP	Management Netmask	Bridge STP	Bridge Priority
1	Management VLAN	1	0	192.168.0.100	255.255.255.0	☐	32768

Interface Membership for Management VLAN:
Add Entry Delete Entry

#	Interface	Type
1	Ethernet Interface	Untagged

VLAN Group 2: Delete VLAN Group 2

#	Name	VLAN ID	VLAN Priority	Management IP	Management Netmask	Bridge STP	Bridge Priority
1	Operations	10	0	192.168.2.100	255.255.255.0	☐	32768

Interface Membership for VLAN Group 2:
Add Entry Delete Entry

#	Interface	Type
1	Ethernet Interface	Tagged
2	Wireless Interface	Untagged

Figure 64 Example 1 Configuration

Example 2: Multiple Wireless Interfaces

Another very desirable VLAN configuration for a wireless device is to support multiple virtual wireless networks. For example, consider a corporate facility where separate networks may be provided for a) permanent staff, b) guests, and c) production network. Each of the three virtual networks can be setup using different encryption keys to enhance security. The setup is illustrated below.

Example 2

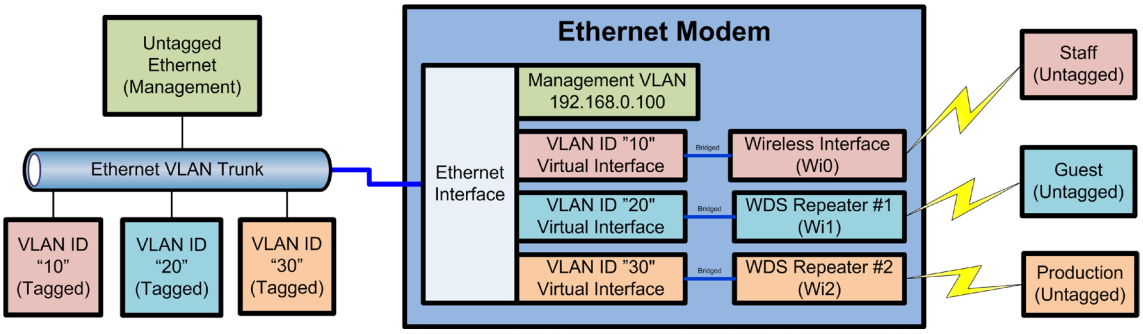


Figure 65 VLAN Example 2

The module is configured with three wireless interfaces. The first one is the normal wireless interface found on the Network page (wi0). The second (wi1) and third (wi2) are virtual interfaces created on the Repeaters page. Each interface is configured as an access point and can be setup with unique SSIDs and encryption settings. In this example, all three wireless interfaces are untagged so that devices joining each of the networks need not be VLAN-aware.

Untagged data from each of the wireless interfaces is individually bridged with one of the three VLAN-aware virtual interfaces “VLAN ID 10,” “VLAN ID 20,” and “VLAN ID 30” on the physical Ethernet interface which forms a VLAN trunk. Untagged data transferred via the first wireless interface (wi0) is internally bridged with the virtual interface VLAN ID 10. Likewise, untagged data transferred via the other two WDS repeater interfaces (wi1 and wi2) are bridged respectively with VLAN ID 20 and VLAN ID 30. The unique VLAN tags are used for corresponding Ethernet data, so that the Ethernet port becomes a VLAN trunk.

Because the 945U-E supports flexible VLAN functionality such that any of the available interfaces can have membership to particular VLAN(s) by assigning membership to one or more VLAN groups—virtually any possible topology can be achieved.

Figure 66 shows the configuration for the multi-VLAN example described above. Notice that there are four groups configured, one for management and one for each of the VLAN IDs. The management group only has the untagged Ethernet interface configured, which means only untagged device on the same IP subnet can access the modules configuration.

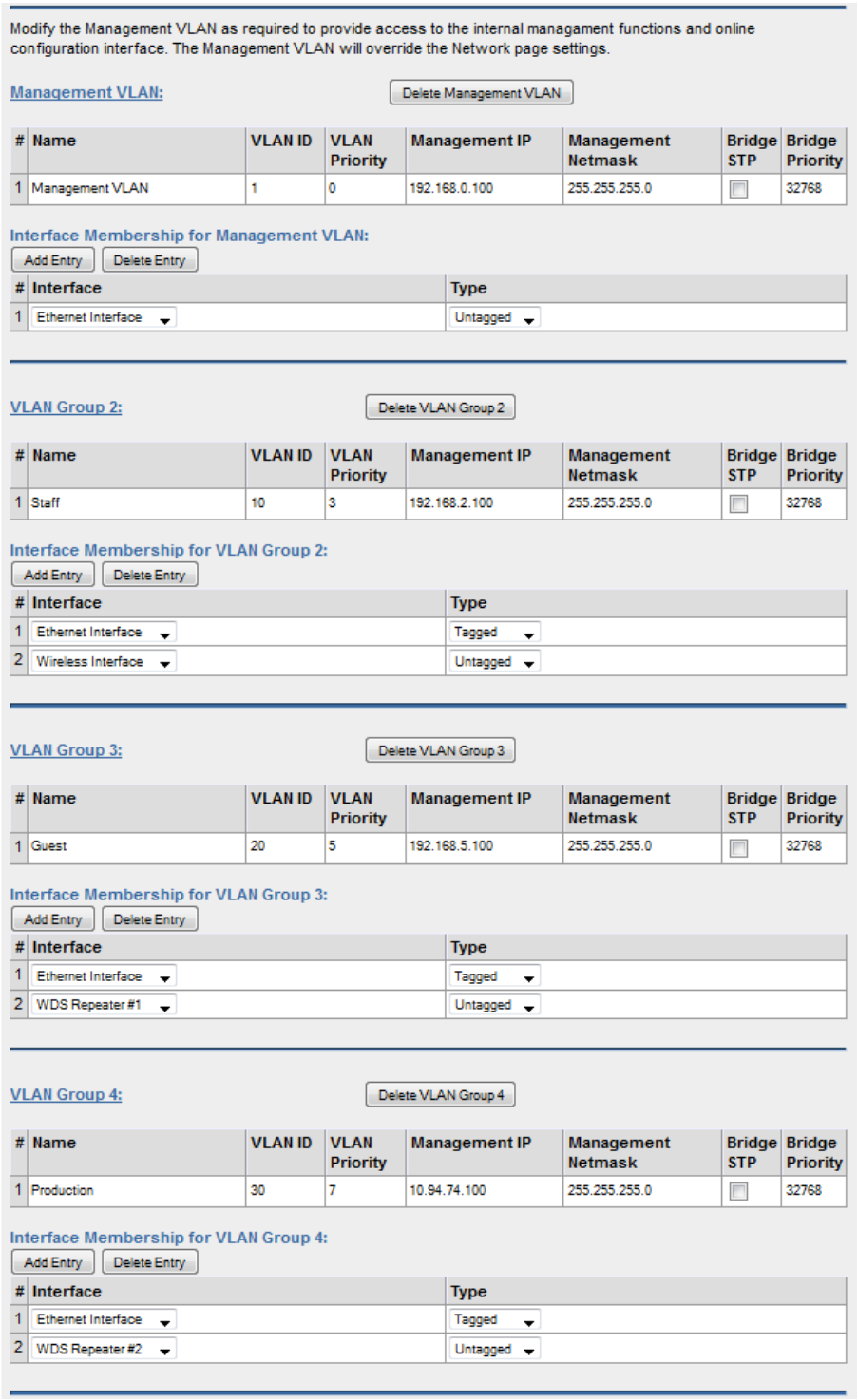


Figure 66 Example 2 Configuration

The other VLAN groups each have an Ethernet and a wireless interface configured. All Ethernet interfaces are tagged because they are all connected to a VLAN network. Each wireless interface is configured as untagged to allow connection from untagged devices. VLAN Group 2 is using the standard wireless interface which is configured from the main network page, while the other two are each using one of the WDS repeater virtual interfaces.

VLAN Group 2 is bridging the default wireless interface with the “VLAN ID 10” virtual Ethernet interface. Configuration of the wireless bridge (operating mode, SSID and radio encryption methods/keys) is performed from the main Network page, as shown in Figure 67.

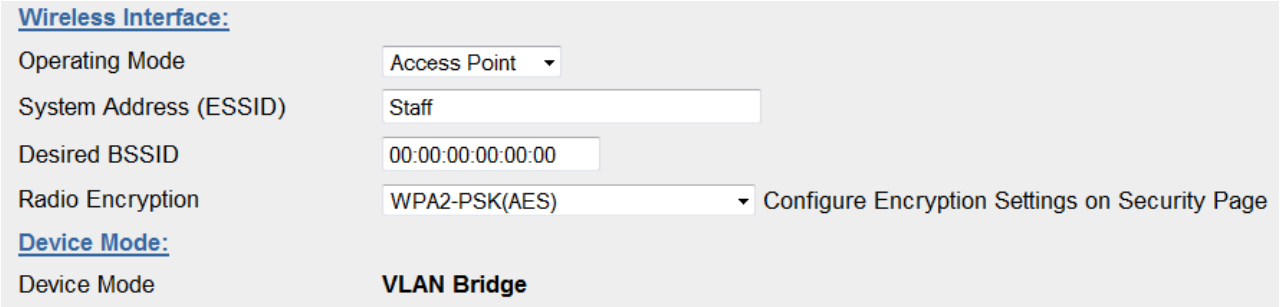


Figure 67 VLAN Encryption

VLAN groups 3 and 4 are similarly bridging their wireless interfaces, but they are using virtual modules that are configured on the Repeaters page. WDS repeater #1 and WDS repeater #2 are being bridged to “VLAN ID 20” and “VLAN ID 30” respectively. Configuration for these wireless bridges is done from the Repeaters page (see the example in Figure 68).

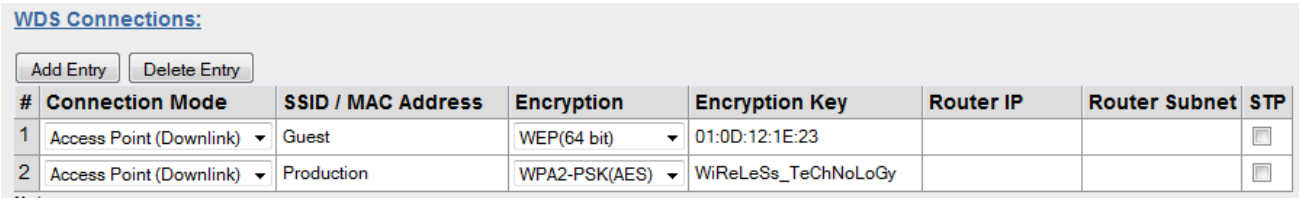


Figure 68 WDS Encryption

Notice that all three wireless interfaces are setup as access points, but are configured with different SSIDs and encryption methods/keys. If encryption fields are left blank, the connection will use the default wireless interface parameters, as configured on the Network page. Similarly, if the router IP and subnet are left blank the connection will use the same default settings.

NOTE Router IP and subnet do not need to be configured in WDS Connections because it will use the IP address assigned in the VLAN group.

The VLAN multiple wireless interfaces example above shows that each group is using a different VLAN priority. Priorities can be given to each interface by configuring a value between zero and seven (seven being the highest priority and one being the lowest). These values can be used to prioritize the configured VLAN networks. In our example, the “Production” VLAN has the highest priority, which means it will have more time slots available to send data, followed by the “Guest” network, and then “Staff.” The default value is zero, which will configure the group to have a mid-range “best effort” value.

3.23 Module Information Configuration

Module Information Webpage Fields

This configuration page is primarily for information purposes. With the exception of the password, the information entered here is displayed on the Home configuration webpage of the 945U-E.

Username	The username used to access the configuration on the 945U-E. Take care to remember this username if you change it, as it will be needed to access the 945U-E in future.
Password	The password used to access the configuration on the 945U-E. Take care to remember this password if you change it, as it will be needed to access the module in future.
Device Name	A label for the particular 945U-E. This is also the DNS name (hostname) of the device if you are using DNS.

Owner	Owner name.
Contact	Owner contact information (such as phone number and email address).
Description	Description of the purpose of the unit.
Location	Location description for the 945U-E.

3.24 Configuration Examples

Setting a 945U-E to Factory Default Settings

1. Access configuration webpages on the 945U-E.

   For details, see “3.2 Configuring the Unit for the First Time.”

2. Click the **System Tools** menu item.
3. Click **Factory Default Configuration Reset**, and wait for the unit to reset.

   While the module executes the reset sequence the OK LED will flash. The OK LED will turn green when the reset sequence is complete.

Extending a Wired Network

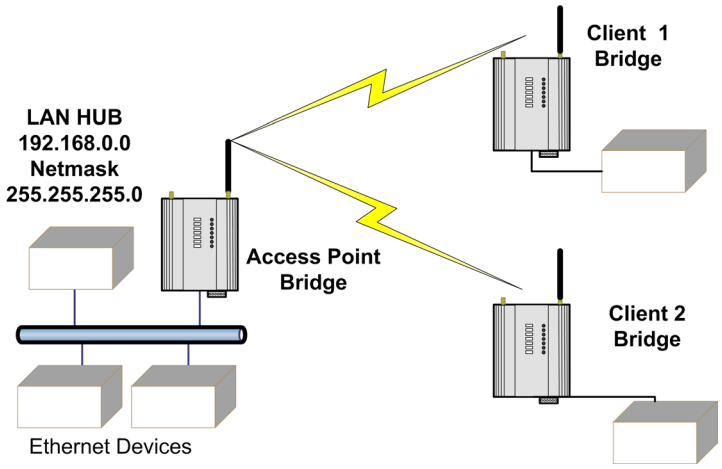


Figure 69 Example Configuration 1

Access Point Configuration

1. Connect a straight-through Ethernet cable between the PC and the 945U-E.
2. Ensure that the configuration of the PC and the 945U-E are setup to communicate on the same network.
3. Set DIP switch to SETUP mode.
4. Power up the unit and wait for the OK LED to stop flashing.
5. Adjust the PC network settings.
6. Set Configuration PC network card with the network setting of IP address 192.168.0.1, netmask 255.255.255.0.
7. Open configuration webpage with Internet Explorer at address 192.168.0.1XX/, where “XX” is the last two digits of the module’s serial number.
8. When prompted for password, enter default username “user” and password “user.”
9. Click **Network** and select Operating Mode as “Access Point.”

10. Select Device Mode as “Bridge.”
11. Change the Gateway IP Address to 192.168.0.1.
12. Change the Ethernet and Wireless IP Addresses to 192.168.0.200.
13. Change Ethernet and Wireless Subnet Masks to 255.255.255.0.
14. Enter a System Address (ESSID) string.
15. Select the radio encryption required.
16. Set DIP switch to RUN.
17. Save the changes.

    The unit will restart with new settings.

Client 1 Configuration

1. Perform the same configuration steps as the access point configuration, with the following differences:
2. Set the Ethernet and Wireless IP addresses of 945U-E to 192.168.0.201
3. Set the Operating Mode to “Client.”
4. Ensure the ESSID and radio encryption method match the access point.
5. If encryption is used, ensure the encryption keys or passphrase match the access point.

Client 2 Configuration

Same as client 1 configuration, except set the Ethernet and wireless IP addresses as 192.168.0.202.

Connecting Two Networks Together

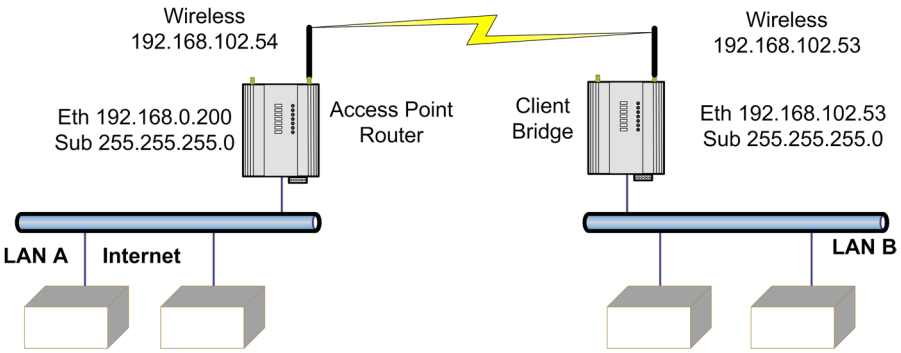


Figure 70 Example Configuration 2

LAN A Configuration

In this example, network A is connected to the Internet via a router at IP address 192.168.0.1. Devices on LAN A that only require access to devices on LAN A and B, should have their gateway IP address set to the 945U-E access point as 192.168.0.200.

Devices on LAN A, that must interact with devices on LAN A and B and the Internet should set the Internet router 192.168.0.1 as their gateway, and must have a routing rule established for devices on network B. On PCs this may be achieved with the MS-DOS command ROUTE. For this example, use ROUTE ADD 169.254.102.0 MASK 255.255.255.0 192.168.0.200. For more information on the DOS “Route” command, see “4.10 Utilities.”

LAN B Configuration

All devices on LAN B should be configured so their gateway IP address is that of the 945U-E access point as 169.254.102.54

Access Point Configuration

1. Connect a straight-through Ethernet cable between the PC and the 945U-E.
2. Ensure that the configuration PC and 945U-E are setup to communicate on the same network.
3. Set the DIP switch to SETUP.
4. Power up the unit, and wait for the LINK LED to cease flashing.
5. Adjust the PC network settings.
6. Set the Configuration PC network card with the network setting of IP address 192.168.0.1, netmask 255.255.255.0.
    a. Open the Configuration webpage with Internet Explorer at address 192.168.0.1XX/.
    b. When prompted for the password, enter default username “user” and password “user.”
    c. Enter “Network” and select the Operating Mode as “Access Point.”
    d. Set the Device Mode to “Router.”
    e. Set the Gateway IP Address to 192.168.0.1.
    f. Set the Ethernet IP Address to 192.168.0.200, network mask 255.255.255.0.
    g. Set the Wireless IP Address to 169.254.102.54, network mask 255.255.255.0.
    h. Select the Radio Encryption required, and enter encryption keys or passphrase if necessary.
    i. Set the DIP switch to RUN.
    j. Click **Save to Flash and Reset**.

        The webpage will display a message indicating details are being written to flash.
7. Wait for the 945U-E to reboot before removing power. Enter a system generator string.

Client Configuration

Perform the same configuration steps as for the access point configuration, with the following differences:

1. Enter “Network” and select Operating Mode as “Client.”
2. Set the Device Mode to “Bridge.”
3. Set the Gateway IP Address to 169.254.102.54.
4. Set the Ethernet IP Address to 169.254.102.53, network mask 255.255.255.0.
5. Set the Wireless IP Address to 169.254.102.53, network mask 255.255.255.0.
6. Click **Save to Flash and Reset**.

    The webpage will display a message indicating details are being written to flash. Wait for the 945U-E to reboot before removing power.

Extending Network Range with a Repeater Hop

Configure units as described in “Extending a Wired Network.” Place the access point at the remote intermediate repeater location. Additional repeaters can be added using wireless distribution system (WDS). Refer to “3.16 Repeaters (WDS)” for details.

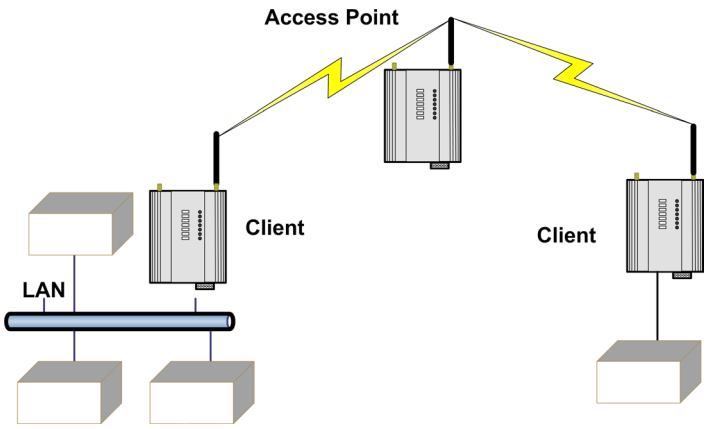


Figure 71 Example of Repeaters

CHAPTER 4 - DIAGNOSTICS

4.0 Diagnostics Chart

LED Indicator	Condition	Meaning
OK	Green	Normal operation.
OK	Red continuously	Supply voltage too low or internal module fault.
OK	Red at Power On	Boot loader delay at startup.
OK	Fast flash Red / Green	Module boot sequence.
OK	Slow flash Red / Green	Module boot sequence.
Radio RX	Green flash	Radio receiving data.
Radio RX	Red flash	Radio receiving data (low signal strength).
TX/LINK	Green	Connection established to remote device.
TX/LINK	Red Flash	Radio transmitting.
RS-232	Green flash	Data sent from RS-232 serial port.
RS-232	Red flash	Data received to RS-232 serial port.
LAN	On	Link established on Ethernet port.
LAN	Flash	Activity on Ethernet port.
RS-485	Green flash	Data sent from RS-485 serial port.
RS-485	Red flash	Data received to RS-485 serial port.
DIO	Green	Digital input is grounded.
DIO	Red	Digital output is active.
DIO	Off	Digital output is Off and input is open circuit.

The green OK LED on the front panel indicates correct operation of the unit. This LED turns red on failure, as described above. When the OK LED turns red, shutdown state is indicated. On processor failure or on failure during startup diagnostics, the unit shuts down and remains in shutdown until the fault is rectified. During module boot-up, the OK LED flashes red-green until the boot sequence is complete.

Boot Status LED Indication During Startup

The OK LED indicates the status of the module during the boot up process. At power on, the OK LED comes on red. During kernel boot, the OK LED flashes red-green at a 1-Hz rate (1/2-second red, 1/2-second green). During module initialization, the OK LED flashes red-green at 0.5-Hz rate (1-second red, 1-second green). When initialization is complete, the OK LED switches to green continuously.

If the OK LED remains red at power on, this could indicate either low supply voltage (the module will not attempt to boot until supply voltage is within range), module fault, or a long boot delay. To check if the boot delay is the problem, plug a terminal into the RS-232 serial port and configure for 115,200 baud, 8 data, no parity.

4.1 Connectivity

The Connectivity webpage displays connections and available networks. The “Connected Devices” section displays the radio channel, received signal strength, and radio data rate for each client or access point by their MAC address. The readings shown are based upon the last received data message from the access point or client. Client stations also display a list of detected access points (site survey), including network name (SSID), channel and maximum data rate.

NOTE When updating the Connectivity webpage, it is necessary to hold down the CTRL key while clicking Refresh, otherwise the information will not be updated.

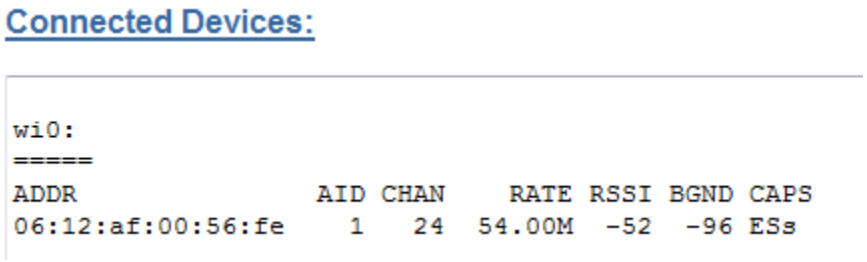


Figure 72 Connected Devices

Connectivity Parameters

AID	Association ID. Every client receives a unique temporary ID from the access point.
CHAN	The radio channel being used.
RATE	Radio data rate.
RSSI	Radio signal strength index (amount of received signal strength).
BGND	Background interference level, in dBms. The amount of internal noise the radio is able to hear. This level does not indicate external radio interference noise level.
CAPS	Capabilities (Ref 802.11 Standard).

Site Survey

Site survey is a one-off snapshot showing the access points that are available for connection. This list is only available on clients, and only available at start up of the module or by selecting “Background Scanning” on the Radio page.

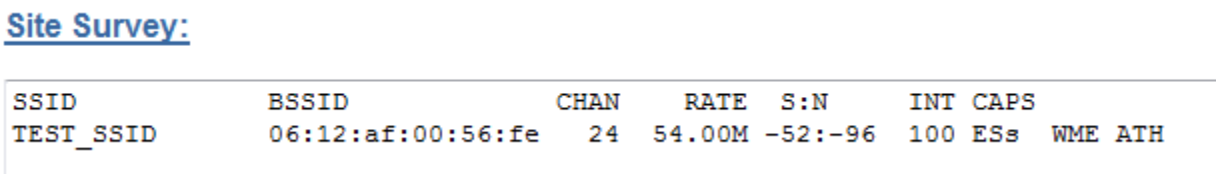


Figure 73 Connectivity/Site Survey

SSID	The service set identifier or network name used to identify a particular network.
BSSID	The MAC (media access control) address of the access point.
CHAN	The radio channel being used.
RATE	Maximum radio data rate.
S:N	Signal strength and noise level. In the case shown in Figure 73, the signal is -44 dB and background noise level is -88 dB.
INT	Beacon interval.
CAPS	Capabilities (Ref 802.11 Standard).

4.2 Channel Survey (Utilization)

Channel utilization gives a visual display of how busy the current channel is over a given time period. Channel utilization is made up of three components—transmissions made by this radio, data received by this radio, and noise or interference that this radio can hear. These three components may also be viewed individually on the Custom Survey page. Channel utilization is logged by the radio for three separate time intervals—every second for

the last 60 seconds, every minute for the last 60 minutes, and every hour for the last 60 hours.

The ELPRO 802.11 Ethernet modem utilizes a half-duplex radio channel for communications. At any given time, an access point and its associated clients occupy a radio channel. These radio channels or frequencies are license free, and may contain interference from any number of other radio transmitters. When installing or diagnosing a 945U-E modem, the potential capacity of a given radio channel will be reduced by the existence of these other RF signals on the same channel.

Channel utilization allows us to see how much RF activity is on a given channel as a percentage of the total utilization. A channel that is very busy will have high channel utilization (usually 50% or greater). Conversely, a channel that is quiet will have low channel utilization.

Channel Survey and Custom Survey can therefore be valuable tools to use when performing site surveys in order to determine the best RF channel to use. It is also a valuable diagnostics tool for identifying the spare capacity on a given channel, as well as possible sources of interference.

Channel Utilization on a Live System

Channel utilization can be used on a live system to get an indication of how much spare capacity the channel has for additional data transfer. To identify possible interference on the current channel, observe the Percent Busy and Percent Rx on the Custom Survey page. If possible, also temporarily disable all data transfer on the system. If the channel utilization remains high this will confirm the presence of interference.

Channel Utilization for Channel Selection or RF Path Testing

When used on an inactive system, channel utilization will indicate how quiet the current channel is and therefore indicate how much interference is present. To select the quietest channel, configure the radio as an access point with no data transfer, and on each channel of interest record the channel utilization over a period of time. The channel with the lowest channel utilization will be the quietest channel and therefore likely to provide the best performance. This procedure, in addition to the throughput test, is recommended for complete radio path testing.

Diagnosing Low Throughput

When Iperf throughput testing has given poor results, channel utilization can be used to confirm whether or not the poor results were due to interference. If the channel utilization (excluding the time period while Iperf was running) is seen to be high, then this will confirm that the poor throughput was due to other RF interference. Alternatively, if the channel utilization is seen to be low (indicating little interference), the poor throughput is more likely be attributed to poor RSSI, which could be confirmed on the Connectivity page.

Solutions for High Channel Utilization

When substantial interference has been identified using Channel Survey or Custom Survey, the simplest solution is to change to another channel that is seen to have lower channel utilization. If a better channel is not available, configuring a fixed noise floor can often greatly improve performance. Configuring a fixed noise floor can be performed on the Advance Radio Configuration page. The fixed noise floor should be at least 8 dB greater than the weakest RSSI of any connected modem, otherwise communications could be lost. After configuring the fixed noise floor, confirm that the channel utilization has dropped to a desirable level, and where possible perform a throughput test to confirm acceptable performance.

The Channel Survey screen displays a graph showing the percentage of time that a channel is being utilized by any of the following causes:

- The connected modem is transmitting.
- The connected modem is receiving valid data from another modem.
- The connected modem has detected RF noise or interference.

Channel Survey shows the channel utilization and noise floor graph with 1-second, 1-minute and 1-hour periods. Figure 74 shows a percent of the overall radio traffic on the channel that is currently being used.

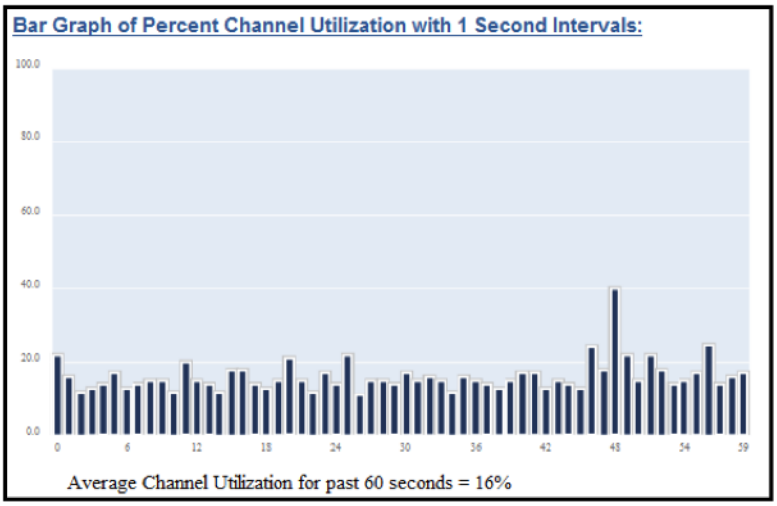


Figure 74 Channel Utilization

Figure 75 shows the radio receive noise floor for the last 60 seconds.

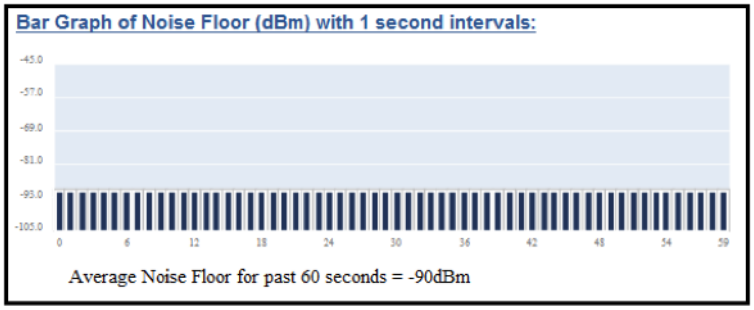


Figure 75 RX Noise Floor

Figure 76 shows the average channel utilization for each minute up to one hour. It will also give a running average for the total number of minutes up to 59 minutes.

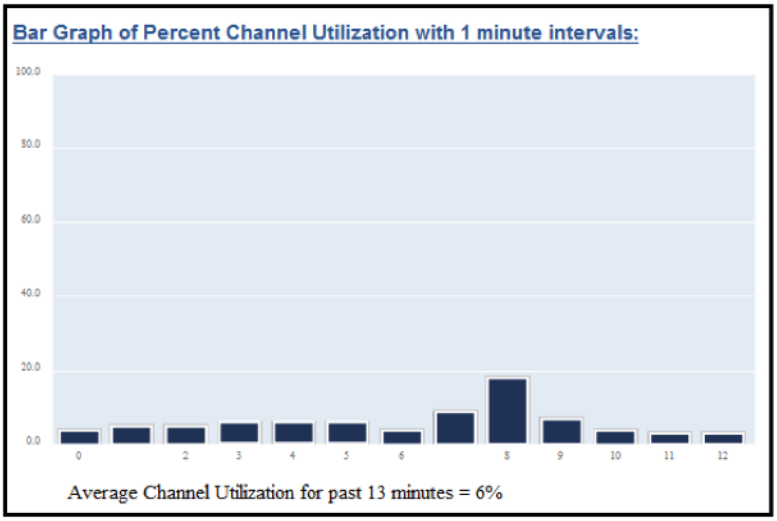


Figure 76 Channel Utilization Minutes

Figure 77 shows the running radio receive noise floor average for each minute up to 59 minutes.

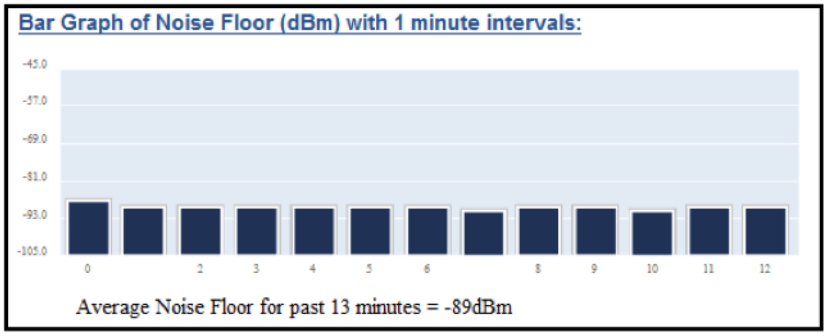


Figure 77 RX Noise Floor Minutes

The Channel Survey page also shows two other screens not shown here that indicate the percent channel utilization and noise floor in one-hour intervals. The screens will only show the last 24-hour period.

4.3 Custom Survey

Custom Survey is essentially the same as the Channel Survey (explained in the previous section), except that the three channel utilizations can be turned on or off, showing the different amount of traffic-related data.

Percent Radio TX	Any transmitted messages from the radio to other devices.
Percent Radio RX	Any DSSS messages received by the radio (basically any radio data from either ELPRO or competitor radios).
Percent Busy (CCA or Noise)	Clear channel assessment (CCA) is the detection of any ongoing transmissions or noise, for example, from devices such as wireless I/O, 900 MHz FHSS, cordless phones, or RC devices.

By configuring the different chart options, you can get a clear idea of the amount of data being transmitted and received, and the amount of other noise that can be heard at the radio. Configure what is to be logged on each chart, select a time interval and save changes, and the charts will then be displayed below the settings. Click the button again to manually redraw the graphs. Each graph will display a percent channel utilization using the selected criteria and time interval (seconds, minutes or hours).

Example 1

In Figure 78, chart one shows the amount of data that is being transmitted over a radio link, and chart two shows the amount of data being received from all sources (interference and other noise). Notice that there is very little outgoing data, but you can see a constant stream of data being received.

Figure 78 Custom Survey 1

Example 2

In Figure 79, notice that chart one shows the amount of data being received from Wi-Fi devices, and chart two shows the amount of other noise that is being received. From this you can see that in the last 60-second period there was a 20-second interval with around 60-80% channel utilization, in this case from another 900-MHz device.

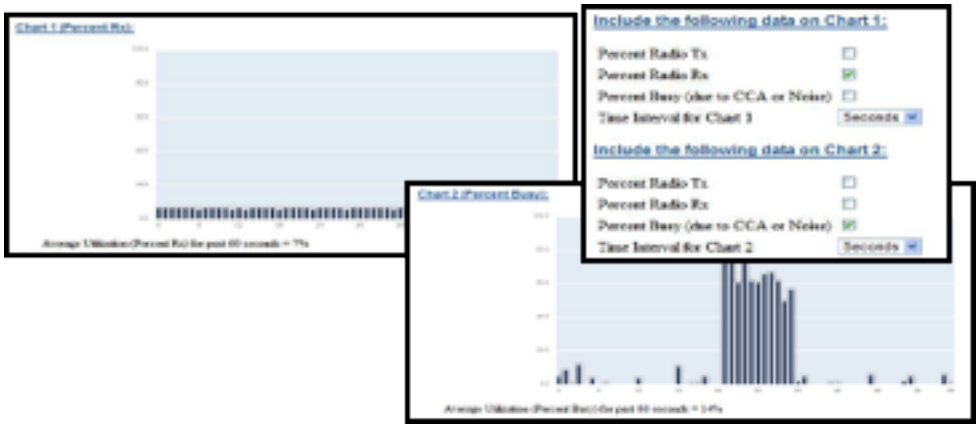


Figure 79 Custom Survey 2

With this type of outside interference, it is recommended to perform the same test over a longer period in order to get a clearer indication of channel utilization.

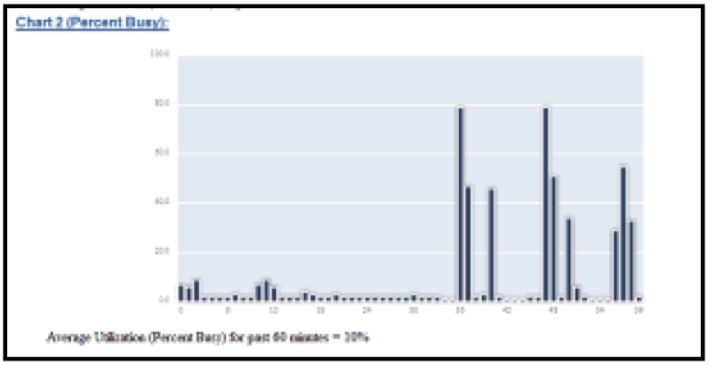


Figure 80 Channel Utilization

4.4 Throughput Test

The performance of a wireless link is best measured in terms of the maximum throughput that can be achieved. The recommended method of measuring throughput is with the “Iperf” utility. Iperf has client and server functionality, where the server waits for a client connection. For wireless links, it is recommended that Iperf throughput testing is performed on point-to-point links, while the remainder of the wireless network is inactive (not sending any data).

The Iperf utility is built into the modems for convenience, and allows measurement of TCP throughput with default Iperf parameters. The internal Iperf utility always gives a lower result than running Iperf externally because of the additional load placed on the internal microprocessor. Even so, the throughput results still gives an excellent indication of link performance as long as you compare the measured result against the expected result in the table. See “3.9 Advanced Radio Configuration” for details on running this application externally.

Internal Throughput Test

Before testing, ensure that the end node of the Wi-Fi link that you wish to test has the Iperf server enabled under the Advanced Radio Settings page and Saved to Flash, and the module has been reset. See “3.9 Advanced Radio Configuration.”

NOTE TCP Throughput test must be run using Microsoft Internet Explorer 8 or later.

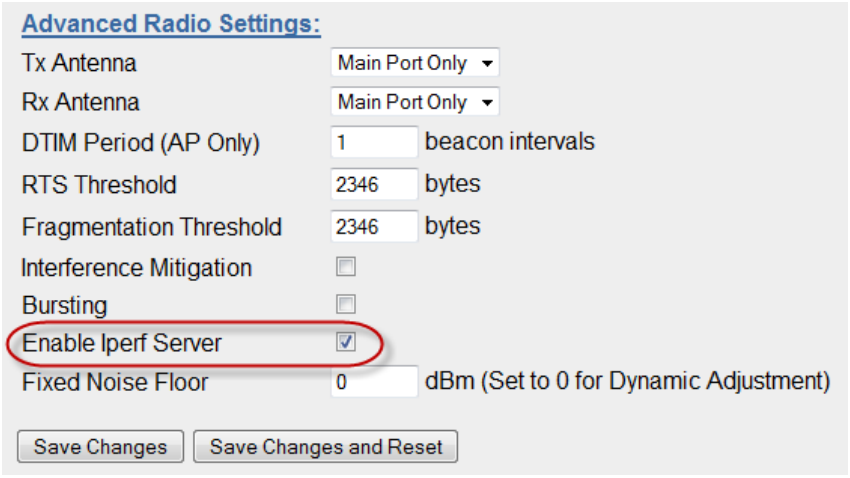


Figure 81 Throughput Test Configuration

To run an internal throughput test:

1. Connect to the webpage of the module that will be performing the Iperf test.
2. Select the “System Tools” link on the right pane of the webpage, and then select “TCP Throughput Test.”

   The screen shown in Figure 82 appears.

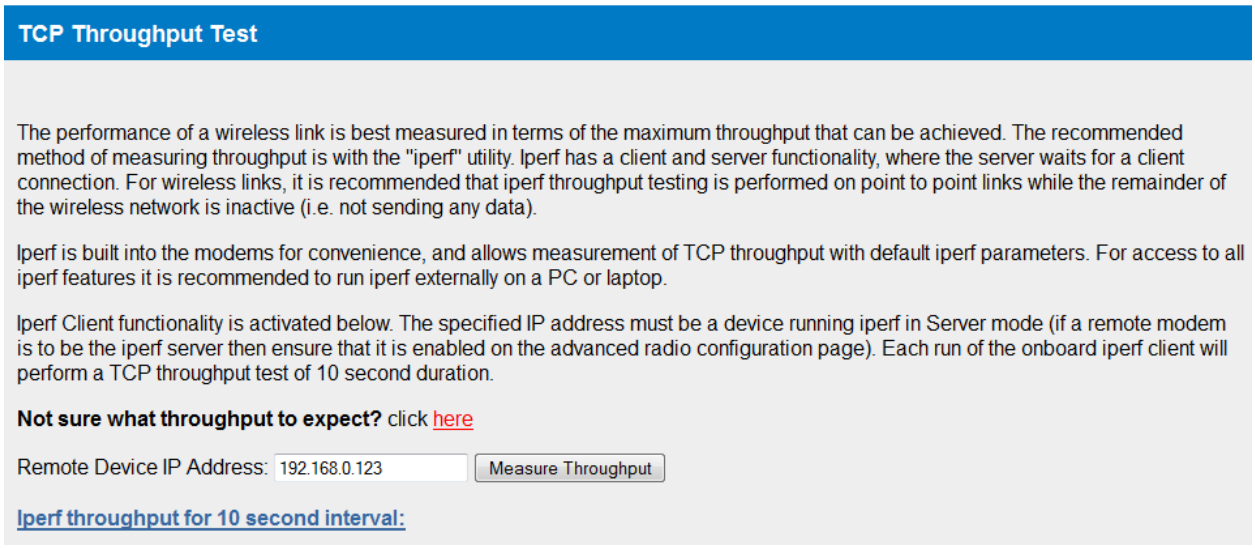


Figure 82 Throughput Test

3. Enter the IP address of the remote device that you wish to test, and click **Measure Throughput**.

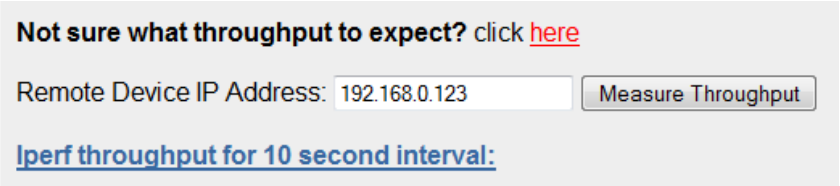


Figure 83 Iperf

The specified IP address must be running Iperf in Server mode (if the remote modem does not have the Iperf server running, you will get the Error message “Iperf error, check connectivity to server.” Ensure that it has been enabled and reset the module. Each time you click Measure Throughput, a 10-second TCP throughput test is performed.

You will see the message “Performing Iperf Test,” and if you look at the modules you will see the TX/Link and RX LEDs flashing quickly as it performs the test. After about 10 seconds, a graph appears showing the actual throughput over the 10-second period and a calculated average.

The graph below shows the data throughput range between 8 and 14.5-Mbits per second with an overall average of 10.9-Mbits per second. It is recommended to perform this throughput test a number of times to get a better sample of the overall throughput.

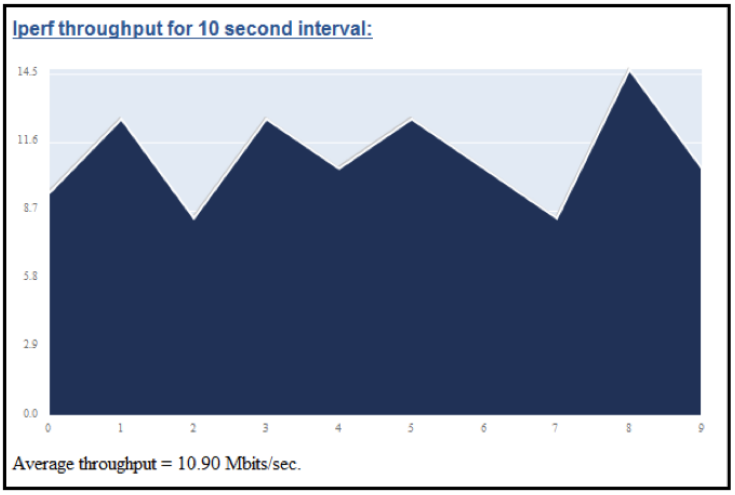


Figure 84 Iperf Throughput

The expected throughput will depend on a number of things, including the distance setting, selected channel width, and whether you are using the internal Iperf utility or running Iperf externally on a laptop or PC (at both ends of the link). The following table shows the estimated throughput results based on real world communications. These estimates are not necessarily the maximum that are achievable in the modems, but are used more as a guideline to determine the performance of the radio link.

The Iperf throughput result provides an excellent measure of the performance of a radio link. In general, if the results you get are much worse than the best case values listed below it is a certain indication that the radio link has either poor RSSI, or high noise or interference, or both. For RSSI or Received Signal Strength Indication, see “4.1 Connectivity.” For information on checking interference or noise, see ”4.2 Channel Survey (Utilization).”

Distance Setting	Iperf Location	20 MHz Channels	10 MHz Channels	5 MHz Channels	2.5 MHz Channels	1.25 MHz Channels
1000 m	Internal	10.5 Mbps	7.5 Mbps	5. Mbps	2.4 Mbps	1.4 Mbps
1000 m	External	16. Mbps	10.5 Mbps	6. Mbps	2.8 Mbps	1.5 Mbps
3000 m	Internal	10. Mbps	7. Mbps	4.7 Mbps	2.4 Mbps	1.4 Mbps
3000 m	External	15. Mbps	9. Mbps	6. Mbps	2.7 Mbps	1.5 Mbps
5000 m	Internal	9. Mbps	6. Mbps	4.5 Mbps	2.3 Mbps	1.4 Mbps
5000 m	External	13. Mbps	8. Mbps	6. Mbps	2.6 Mbps	1.5 Mbps
10000 m	Internal	7. Mbps	5. Mbps	4. Mbps	2.2 Mbps	1.3 Mbps
10000 m	External	10. Mbps	7. Mbps	5. Mbps	2.4 Mbps	1.4 Mbps

4.5 Statistics

The Statistics webpage is used for advanced debugging of 945U-E. This webpage details the state of the 945U-E and performance information. This page is typically useful to ELPRO technical support personnel in diagnosing problems with the module.

NOTE When updating the Statistics webpage, it is necessary to hold down the CTRL key while clicking Refresh, otherwise the information will not be updated.

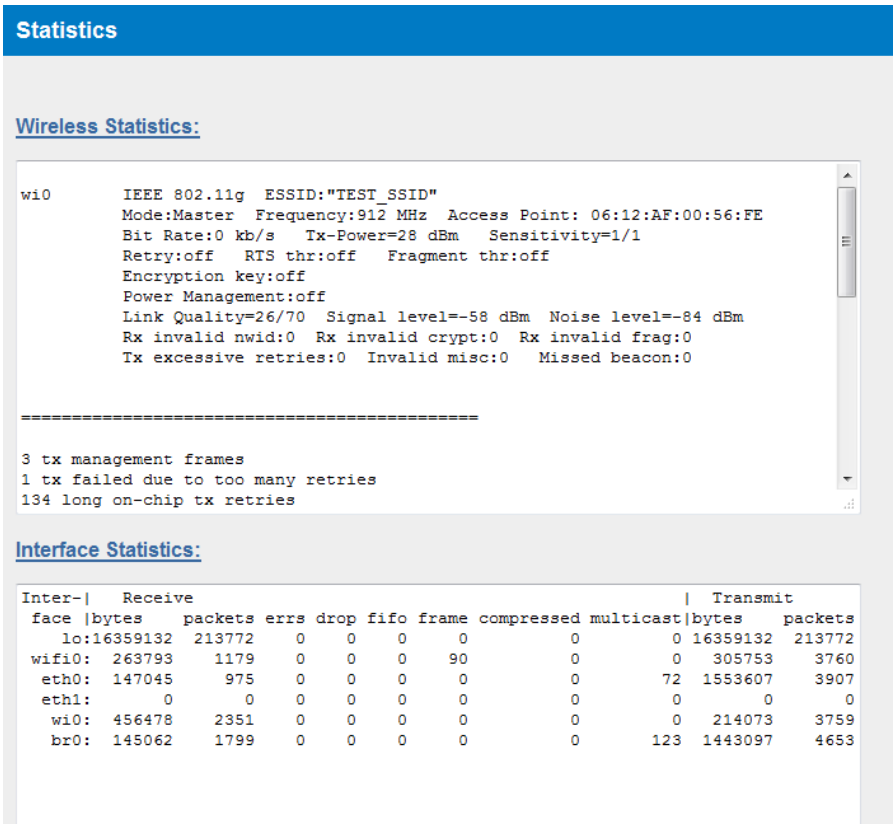


Figure 85 Statistics

Wireless Statistics

The “Wireless Statistics” pane on the Statistics page shows further diagnostics statistics. The list of statistics produced is dynamic and may vary depending on the model and configuration (2.4 GHz, 5 GHz or 900 MHz, and Client or Access Point).

Access Point

Beacon Miss Count	Number of beacons unable to be sent (100-msec intervals) due to interference or CCA.
Beacon Missed Reset Count	After 15 consecutive beacon misses (1.5 seconds), this count will increment by 1. This will indicate high interference as the access point is holding off sending beacon and utilization will increase.
TX Queue stopped because full	Message buffer (Ethernet Frames) in radio queue. If the radio cannot transmit due to high noise, this will increment. When the buffer is full, all new messages are dropped. Buffer size is 150 messages.

Client

Beacon Missed Interrupts	The number of beacons (100 msec) the client has missed from the access point.
TX Failed due to too many retries	The number of frames that have been lost. Original Message + 7 Retries = 1 TX Failed due to too many retires. Each retry is sent within a few milliseconds. TX Failed / TX Antenna Profile = Frame Packet Loss Rate (number of undelivered, as a percentage).
RX Failed due to bad CRC	This can be from any access point, not only your own. If other Wi-Fi networks are in the area, this number could be high due to other encryption keys or weak signal. RX Failed / RX Antenna Profile = RX Frame Error Rate (this can be high due to other wireless devices in the area).
Broadcast Notes	When a broadcast message is sent from the client to the access point, the access point will always ACKnolwedge the client. When a Broadcast Message is sent from access point to the client, no ACK will be sent back.
Management Frames	Can be probes, authenticate/associate messages, RTS messages, beacons, and so on.

Network Traffic Analysis

There are many devices and PC programs that will analyze performance of an Ethernet network. Freely available programs ,such as Ethereal, provide a simple cost effective means for more advanced analysis. By monitoring traffic on the wired Ethernet, a better idea of regular traffic can be discovered. Network Analysis programs make configuration of a filter for the 945U-E a simple task.

4.6 System Tools

The System Tools Page has a number of tools that help maintain the module firmware and configuration.

Configuration Summary	This option is used to save all the different Configuration pages onto one page for easy viewing. Page can also be saved (using the File/Save As function on the drop File Menu) for future reference, and emailing module configuration details to ELPRO technical support in the event of any configuration problems.
TCP Throughput Test	Perform a throughput test. See “4.4 Throughput Test” for details.
Radio Path Test	Perform a radio path test without the use of a laptop and get a visual indication of RSSI and throughput on the front panel LEDs.
Read Configuration File	This option will show the module configuration in XML format. This file can be saved for future reference.
Write Configuration File	Any configuration XML files saved using the “Read Configuration” above can be loaded back into the module.

Firmware Upgrade	This option is used for firmware upgrades. Load the file using the Browse button. When the file is found, click Send to load the file into the module. When completed, click Reset. Firmware upgrade can be executed locally, or remotely via the radio.
System Log File	Shows an event log of the modules operation. Used for diagnosing problems. The page can be saved and emailed to ELPRO if requested. “Clear System Log” will clear the log file and start afresh.
Reset	Resets the module.
Factory Default Configuration	Loads the factory default configuration and resets the module. **CAUTION This will overwrite any current configuration.**

4.7 Testing Radio Paths

Connection and Signal Strength

The general, the procedure for radio range testing a link is fairly simple. Configure two units to form a link using automatic radio rates, and install the access point at a fixed location. Take a laptop computer and the client to each of the remote locations and analyze the link using the Connectivity webpage. If a beacon is heard from the access point, the client will update its Connectivity webpage with the received signal strength of beacon messages from the access point.

If the signal is strong enough, a link may be established and the Connectivity webpage of the access point may be opened. If the link is weak, the LINK LED will turn off and the remote Connectivity webpage of the access point will fail to load. Using this procedure, the signal strengths of units at both locations may be analyzed and traffic is sent between the units while remote webpages are opened.

Throughput Test

A more thorough test of radio paths is a throughput test, which will check the amount of data that can be reliably achieved via the wireless link. There are a number of software tools that you can use to check the data throughput, for example, FTP (file transfer protocol), Iperf, or Qcheck. The preferred application is “Iperf,” which has been configured in each modem and can be enabled to perform this test. It can also be run externally using laptops at either end of the radio link. The Iperf/Jperf application can be downloaded from http://sourceforge.net/projects/iperf/.

All of the above applications measure the raw data throughput. From this you can determine the amount of interference from the measured and calculated data throughput levels. The way Iperf works is that a server is enabled at one end of the link and a client at the other. The Iperf client will then pass data over the link and calculate and display the throughput accordingly. The Iperf server can be run internally on the modem by enabling this feature on the Advanced Radio page of one of the modems (see “4.4 Throughput Test”). It can also be run externally on a PC or laptop connected at each end of the radio link. See “Appendix D - IPERF THROUGHPUT TEST - EXT” for a detailed procedure on how to use Iperf to externally check radio data throughput.

The internal Iperf is a cut down version of the standard Iperf and should be used as a guide only. For a more comprehensive test Iperf should be run externally using laptops or PCs at each end of the Wi-Fi link.

Internal Radio Tests

The module also has an internal radio path test that will allow you to perform a basic radio path test without the need for a laptop or PC. Two tests that can be run—RSSI, and throughput. The throughput test can be disabled independently from the RSSI test, but disabling the RSSI test will turn off both tests. Typically, the radio path test should be enabled at a modem configured as a client or station.

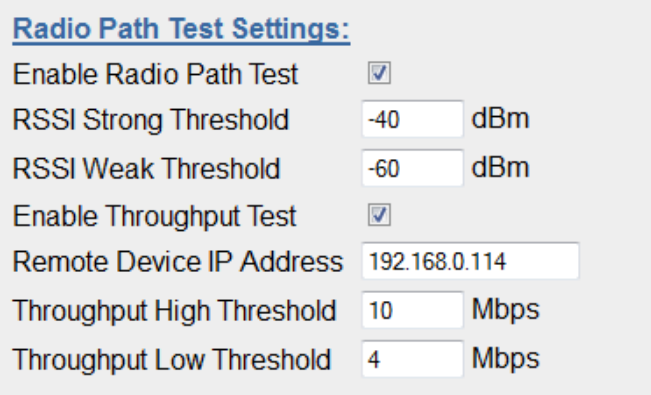


Figure 86 Radio Path Tests

NOTE The Radio Path Test feature should not be enabled on a live system. It is intended for testing only.

Radio path settings are as follows.

Enable Radio Path Test	Enables or disables the radio path test.
RSSI Strong Threshold	Strong RSSI indication threshold.
RSSI Weak Threshold	Weak RSSI indication threshold.
Enable Throughput Test	Enables or disables the throughput test (independent of radio path test (RSSI).
Remote Device IP Address	IP address of the remote device that you wish to path test.
Throughput High Threshold	High throughput indication value. Generally configured with the desired throughput level.
Throughput Low Threshold	Low throughput indication value.

RSSI Test

The first test (RSSI Test) uses the RS232 LED to indicate the RSSI level from the access point. The LED will be green when the RSSI to the access point is greater than the configured RSSI Strong Threshold, or red when the RSSI to the access point is greater than the configured RSSI Weak Threshold. If the RSSI to the access point is less than the RSSI Weak Threshold, the RS232 LED will be off. When the Radio Path Test is enabled, the OK LED will flash alternately between green and red, indicating that it is in a diagnostic mode.

Throughput Test

The second test is the throughput test, which when enabled performs a basic throughput test between the access point and client. The configurable remote device IP address should specify the IP address of the access point.

NOTE The onboard Iperf server must be enabled at the access point prior to running this test.

The throughput test will run through a continuous cycle where data is transferred for 10 seconds, followed by 10 seconds of silence. The RS485 LED and the DIO LED are used as indicators of the throughput test. While data is being transferred the DIO LED is red, and while no data is being transferred the DIO LED is off.

If the average throughput over the 10-second duration of the throughput test is greater than the configurable Throughput High Threshold, then the RS485 LED will be green. Otherwise, if the throughput is greater than the configurable Throughput Low Threshold the RS485 LED will be red. If the measured throughput is less than the

Throughput Low Threshold, the RS485 LED will be off.

Radio path test can be accesses by selecting the link from the System Tools page and then ticking the “Enable Radio Path Test” and entering in appropriate thresholds levels to indicate RSSI and throughput and the IP address of the Iperf server (normally the access point).

Figure 87 shows the indications you will see using the configuration above.

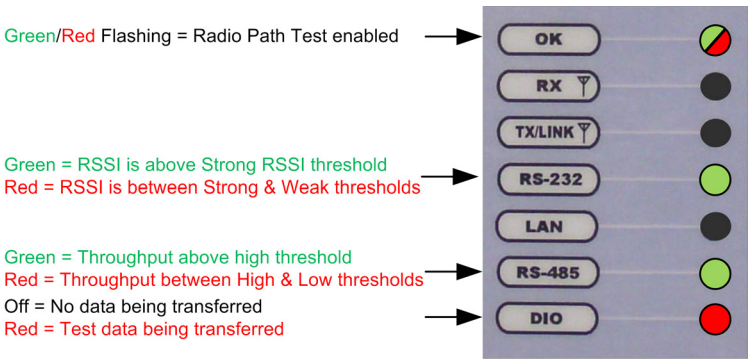


Figure 87 Throughput Test LEDs

- The OK LED will flash between red and green, which indicates the module is in a diagnostic Radio Test mode.
- RS-232 LED is showing a green indication which means the RSSI to the access point is greater than -40dB. If the RS232 LED were red, it would indicate the RSSI level was greater than -60dB.
- RS-485 LED is showing a green indication, which means the throughput to the access point is greater than 10 Mbps. If the LED showed a red indication, this would mean the throughput is between 10 Mbps and 4 Mbps.

NOTE Advanced configuration settings such as Serial or I/O Transfer should be disabled, and if using the throughput test, the Iperf Server option on the Advanced Radio Settings page for the access point must be enabled.

4.8 Remote Configuration

Because a module configuration is viewed and changed in a Web format (which uses TCP/IP protocol), you can view or change the configuration of a remote module via the wireless link, provided the remote module already has a wireless link established to the local 945U-E. To perform a remote configuration, connect a PC to the local module, run Internet Explorer and enter the IP address of the remote unit (or device name if using DNS). The configuration page of the remote module will appear and changes can be made.

NOTE Care must be taken if modifying the configuration of a module remotely. If the radio configuration is changed, some changes made may cause loss of the radio link, and therefore loss of the network connection.

It is advisable to determine the path of the links to the modules you wish to modify and draw a tree diagram, if necessary. Modify the modules at the “leaf nodes” of your tree diagram. These will be the furthest away from your connection point in terms of the number of radio or Ethernet links. In a simple system, this usually means modifying the client modules first and the access point last.

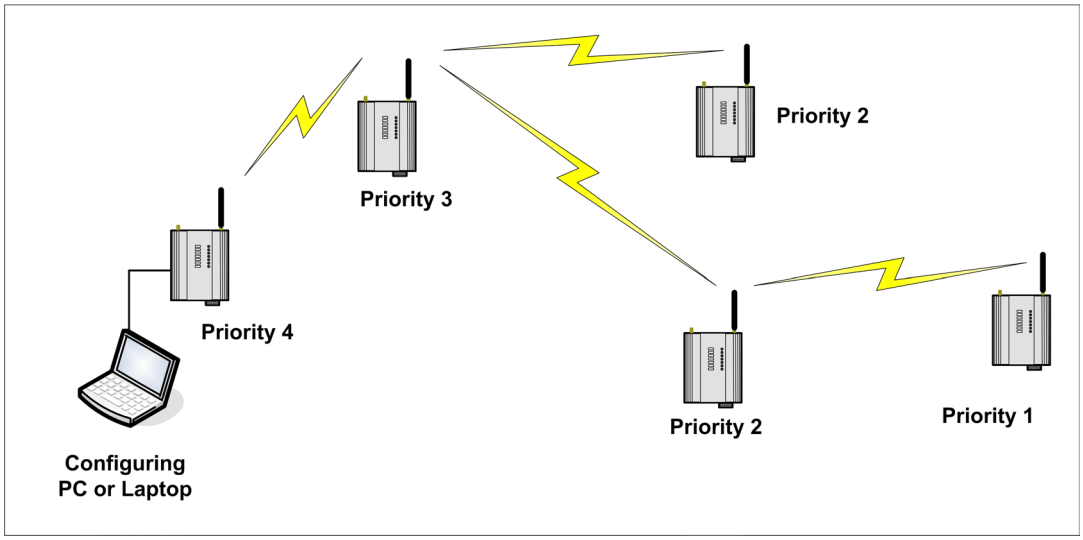


Figure 88 Remote Configuration

4.9 Internal Diagnostic Modbus Registers

There are a number of internal diagnostic registers that can be accessed via Modbus TCP/RTU that will help with analyzing and diagnosing the radio network. To access these registers, the Modbus server will need to be enabled and a Modbus server address will need to be configured. For details, see “3.14 Modbus I/O Transfer.”

After enabling the Modbus client, you can access the following information by reading the corresponding Modbus address at the server ID address.

NOTE The normal default interface is “wi0.” If more interfaces are added by entering in virtual WDS connections (either client or access point) as described in “3.16 Repeaters (WDS),” they will take the next available interface number.

Connection Information

Register	Module	Description
5000	Both	Total number of associated stations.
5001	Both	Current radio channel. See “3.1 Selecting a Channel” for channel details.
5002	Both	Number of wireless interfaces configured, including virtual interfaces (wi1-wi10).
5010	Both	Wireless adapter (wi0) – link status.
5011	Both	Wireless adapter (wi0) – link status inverted.
5012	Both	Wireless adapter (wi0) – number associated stations for this interface.
5013	AP Only	Wireless adapter (wi0) – points to the starting register of the access point’s station list. First interface (wi0) will always start at 5200 and dynamically enter data depending on the number of STAs. Remaining interfaces (wi1-wi10) will be entered after wi0 data. Register 5023, 5033 (and so on) will indicate starting location for each interface.
5014	STA Only	Wireless adapter (wi0)—RSSI and BGND of RX message from the access point. For example, hexadecimal 5F5D = 5D for RSSI and 5F for BGND. (Convert the value from hexadecimal to decimal and add a “-”. For example, 5F = -95dB.)
5015	STA Only	Wireless adapter (wi0) – transmit data rate from the access point.
5016	STA Only	Wireless adapter (wi0) – MAC address of the access point.
5020-5026	As per 5010-5016	As per registers 5010-5016, but for the next wireless adapter (wi1).

Register	Module	Description
5030-5036	As per 5010-5016	As per registers 5010-5016, but for the next wireless adapter (wi2).
5040-5046	As per 5010-5016	As per registers 5010-5016, but for the next wireless adapter (wi3).
.....etc	As per 5010-5016	As per registers 5010-5016, but for the next wireless adapter (wi10).
5200	AP Only	RSSI of the client (STA).
5201	AP Only	Transmit data rate to client (STA).
5202	AP Only	MAC address of client (STA).
.....etc	AP Only	Dynamic list of STAs. Refer to register 5023, 5033 (and so on) for starting register of each wi interface.
9999	Both	Reset module (enter FFFF to reset module).

Statistic Registers

Register	Module	Description
4500	Both	Total data packets received on the interface.
4502	Both	Received frames with antenna 1 (TX/RX).
4504	Both	Received frames with antenna 2 (RX).
4506	Both	Receiver / default antenna switches.
4508	Both	Receive message failed due to bad CRC.
4510	Both	Receive message failed due to decryption.
4512	Both	Receive message failed due to MIC failure.
4514	Both	Receive message failed due to FIFO overrun.
4516	Both	Beacon missed interrupts.
4518	Both	Total data packet sent on the interface.
4520	Both	Transmit frames with antenna 1 (TX/RX).
4522	Both	Transmit frames with antenna 2 (RX).
4524	Both	Transmitter antenna switches.
4526	Both	Transmitter on-chip retries.
4528	Both	Transmit message failed due to too many retries.
4530	Both	Transmit frames with alternate rate.
4532	Both	Transmit frames with no ACK marked (broadcast, multicast).
4534	Both	Management frames transmitted
4536	Both	Transmit frames with RTS enabled.
4538	Both	Transmit frames with CTS enabled.
4540	Both	Beacons transmitted.
4542	Both	Beacon missed count.
4544	Both	Beacon miss reset count.
4546	Both	Transmit message failed due to no TX buffer (data).
4548	Both	Fatal hardware error interrupts.
4550	Both	Receiver PHY error summary count.
4552	Both	Transmitter queue stopped because it is full.

4.10 Utilities

ping

Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer that you are trying to reach is actually operating. For example, if a user can not ping a host the user will be unable to send files to that host. Ping operates by sending a

packet to a designated address and waiting for a response.

The basic operation of ping can be performed by following these steps in any Windows operating system.

1. Click the **Start Menu** and choose **Run**.
2. Type “cmd” and press **Enter**.

   You should see the Command Prompt screen appear. There will be a certain directory specified (unique to your own PC) with a flashing cursor at the end.
3. At the cursor type the word “ping” followed by a space and the default IP address for the 945U-E at first startup.

   This command would be written as “ping 192.168.0.118”. Press Enter to send the ping command.

   The PC will reply with an acknowledgment of the command, and if the 945U-E is correctly configured the reply will look similar to Figure 89.

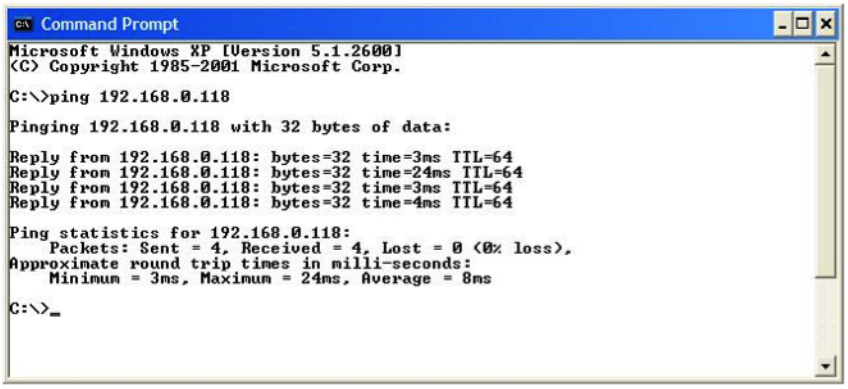


Figure 89 Ping

Figure 90 shows the response of the “ping -t 192.168.0.118” command.

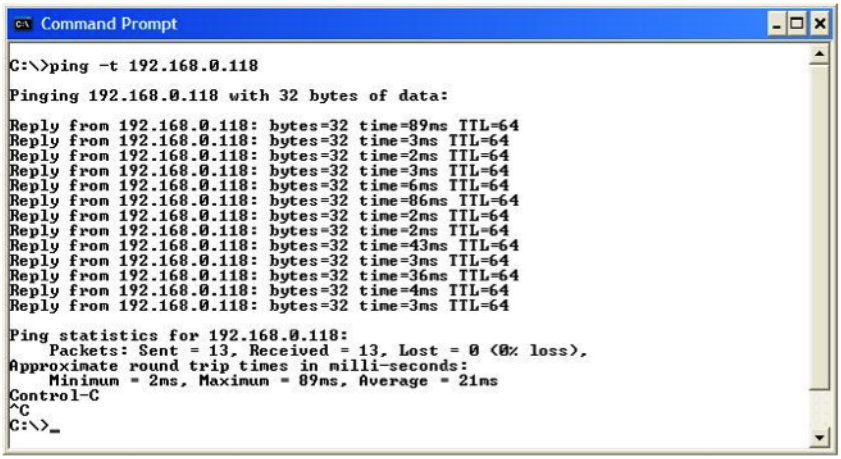


Figure 90 Ping -t

This -t command is used to repeatedly ping the specified node in the network. To cancel use CTRL+C.

A good test for the network once it is first set up is to use Ping repeatedly from one PC’s IP address to the other PC’s IP address. This gives a good indication of the network’s reliability and how responsive it is from point to point. When you enter CTRL+C the program reports a packet sent-received-lost percentage.

ipconfig

The “ipconfig” command can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on.

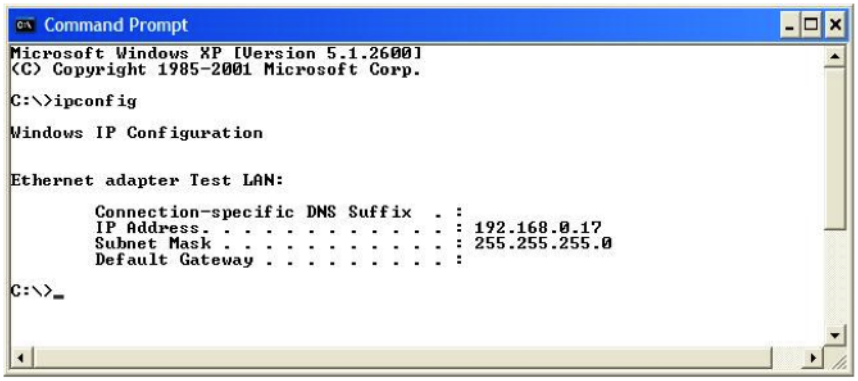


Figure 91 Ipconfig

In the example above, ipconfig was entered in the command prompt. The reply shows the PC’s IP address, subnet mask, and the gateway it is connected to. Other ipconfig commands will return more information. The hardware or MAC address of the computer may be discovered using the command ipconfig /all. The command “Ipconfig /?” lists all of the commands and their usages available for use.

arp

The “arp” command displays and modifies the IP to physical address translation tables used by Address Resolution Protocol (ARP). Once a remote computer has been pinged, this command can be used to see the IP address and MAC address of the remote computer. It will also show any other devices on the network to which it may be connected.

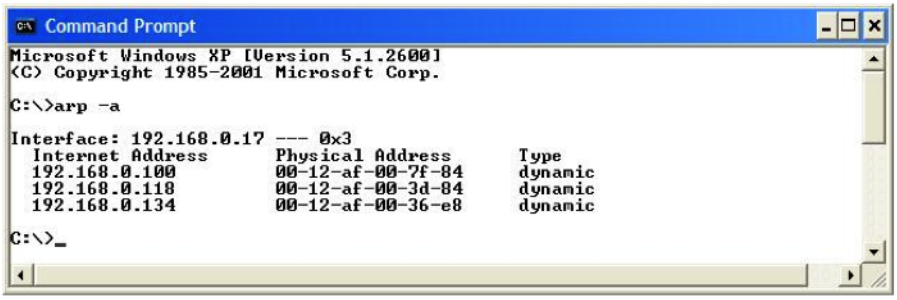


Figure 92 Arp

The command used in the above example is “arp -a”. It shows the PC’s IP address, as did the previous ipconfig command—in this case the IP address is still 192.168.0.17. It also shows the IP address and its associated MAC address of any another device that has a connection to it.

The command “arp -?” lists the commands available for this function.

route

The “route” command is used where you are joining two or more different networks together via the 945U-E. Refer to “1.1 Getting Started Quickly” for details. If more than one routing rule is needed (for example, for multiple networks each with a different IP range), a routing table is required. If only one route is required, a default gateway IP address on the main Network Page can be configured instead of configuring a routing rule.

In the example in Figure 93, a routing rule needs to be entered into the Network A’s PC which will allow access between Network A and Network B. This can be entered at the command prompt using the following instructions.

- route PRINT will show all active routes on PC.
- route ADD will add a routing table to network.
- route DELETE <destination netmask gateway interface> will delete the unwanted routing table.
- route CHANGE modifies an existing route.

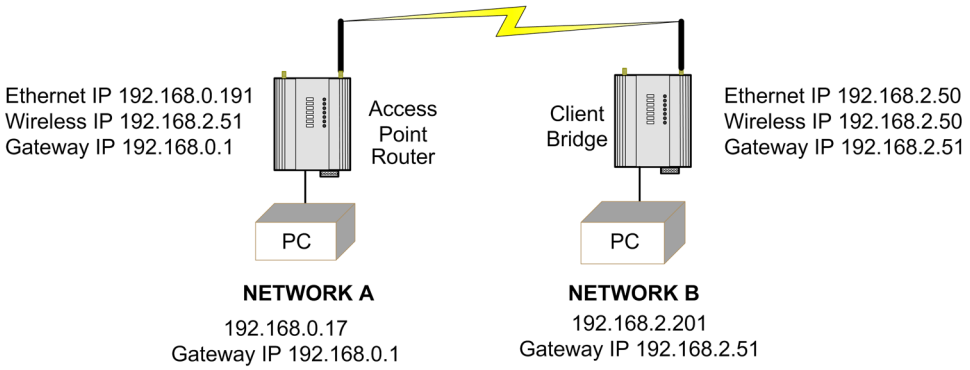


Figure 93 Route

The following is an example of a routing table for the configuration.

Network A Settings
IP Address 192.168.0.17
Subnet Mask 255.255.255.0
Gateway IP 192.168.0.1

Client Bridge Settings
Gateway IP 192.168.2.51
Ethernet IP 192.168.2.50
Subnet Mask 255.255.255.0
Wireless IP 192.168.2.50
Subnet Mask 255.255.255.0

Access Point Router Settings
Gateway IP 192.168.0.1
Ethernet IP 192.168.0.191
Subnet Mask 255.255.255.0
Wireless IP 192.168.2.051
Subnet Mask 255.255.255.0

Network B Settings
IP Address 192.168.2.201
Subnet Mask 255.255.255.0
Gateway IP 192.168.2.51

In the Network A PC a routing rule is to be set.

This will allow Network A and B to have access to each other. This is entered under the command prompt as follows:

Route ADD 192.168.2.0 MASK 255.255.255.0 192.168.0.191

This says access everything on Network B (192.168.2.0) with the mask of 255.255.255.0 on Network A via the Ethernet IP interface 192.168.0.191.

IP address 192.168.2.0 will allow everything on this network to be shared by the router. When adding a routing table you will need to enter this information. Once entered, the router will determine whether to pass information over the router if it is addressed to do so or not. For added security MAC address filtering could be added, as discussed earlier in “3.18 Filtering.”

CHAPTER 5 - SPECIFICATIONS

Transmitter/Receiver	
Frequency	902–928 MHz (1) 915–928 MHz (2)
Transmit Power	250 mW (+24 dBm) to 630 mW (+28 dBm) (data rate and country specific)
Transmission	Direct Sequence Spread Spectrum (900 MHz DSSS)
Modulation	Orthogonal Frequency Data Modulation (OFDM)
Receiver Sensitivity	–95 dBm @ 0.25 Mbps, 71 dBm @ 54 Mbps (8% FER)
Channel Spacing	9 x 1.25 MHz; 9 x 2.5 MHz 4 x 5 MHz; 4 x 10 MHz; 2 x 20 MHz
Data Rate	1–54 Mbps (1) 0.25–27 Mbps (2) Auto mode selects fastest rate possible relative to RSSI
Range (LoS)	12 miles (20 km) @ 630 mW (27 dBm) (3) 18 miles (30 km) @ 1W (30 dBm) (3)
Antenna Connector	2 x Female SMA Standard Polarity (4)
Input/Output	
Discrete I/O	Input Voltage-Free Contact (5) Output FET 30 Vdc 500 mA (5)
Ethernet Port	
Ethernet Port	10/100baseT; RJ45 Connector – IEEE 802.3
Link Activity	Link, 100baseT via LED
Serial Port	
RS232	DB9 Female DCE; RTS/CTS/DTR/DCD
RS485	2-Pin Terminal Block – Non-isolated (6)
Data Rate (Bps)	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 76800, 115200, 230400 Bps
Serial Settings	7/8 Data Bits; Stop/Start/Parity (Configurable)
Protocols/Configuration	
System Address	ESSID; 1 – 31 Character Text String
Protocols Supported	TCP/IP, UDP, ARP, SNMP, RADIUS/802.1x, DHCP, DNS, PPP, ICMP, HTTP, FTP, TFTP, TELNET, MODBUS and MODBUS-TCP
User Configuration	User Configurable Parameters via HTTPS Embedded Web Server
Configurable Parameters	Access Point/Client/Bridge/Router Point-to-Point, Point-to-Multi-point Wireless Distribution System (AP - AP Repeater) Modbus TCP/RTU Gateway Serial Client/Server/Multicast Simultaneous RS232/485 Connection Embedded Modbus Master/Slave for I/O Transfer
Security	Data Encryption – 802.11i With CCMP 128-bit AES Support for 802.1x Radius Server Secure HTTP Protocol

Bandwidth Protection	MAC Address – Whitelist/Blacklist IP Filtering – Whitelist/Blacklist ARP/GARP Filtering – Whitelist/Blacklist
LED Indication/Diagnostics	
LED Indication	Power/OK; RX; TX/Link; RS232; LAN; RS485; Digital I/O status. Please refer to product manual for further information.
Reported Diagnostics	RSSI Measurements (dBm); Connectivity Information/Statistics; System Log file
Network Management	Optional Network Management System
Compliance	
EMC	FCC Part 15; EN 301 489 – 17; AS/NZS CISPR22
RF (Radio)	EN 300 328; FCC Part 15; RSS 210
Hazardous Area	CSA Class I, Division 2; ATEX; IECEx nA IIC
Safety	IEC 60950 (RoHS Compliant)
UL	UL Listed
General	
Size	4.5" x 6.7" x 1.2" (114 mm x 168 mm x 30 mm)
Housing	Powder-Coated Aluminum
Mounting	DIN Rail
Terminal Blocks	Removable; Max conductor 12 AWG (2.5 mm^2)
Temperature Rating	–40 to +140°F (–40 to +60°C)
Humidity Rating	0–99% RH Noncondensing
Weight	1.1 lb (0.5 kg))
Pollution Degree	2 - Not sealed, not subject to dust, dirt, condensation.
Installation Category	2- Transient voltages are not higher than 2.5 kV at 250 Vac supply
Altitude	2000 m
Power Supply	
Nominal Supply	9 to 30 Vdc; Under/Over Voltage Protection
Average Current Draw	300 mA @ 12 V (idle); 160 mA @ 24 V (idle)
Transmit Current Draw	410 mA @ 12 V (27 dBm); 210 mA @ 24 V (27 dBm) 500 mA @ 12 V (30 dBm); 250 mA @ 24 V (dBm)

NOTE Specifications subject to change.
1 Configured for US.
2 Configured for Australia, Brazil.
3 Typical maximum line-of-sight range.
4 Supports signal diversity or high gain antenna.
5 Can be used to transfer I/O status or communications failure output.
6 Maximum distance 1200 meters.

APPENDIX A - FIRMWARE UPGRADES

Determine which firmware version is present in the module to be upgraded by viewing the index webpage of the module. Firmware versions 1.0.3 and later may be upgraded via the Configuration webpages. This upgrade can be performed locally with a PC connected directly to the module, or remotely over a working radio link. For remote upgrades, it is advisable to reduce radio traffic over the link from other devices as much as possible. If necessary, create a temporary separate radio network to perform the upgrade to remote modules.

Web-based Upgrade

Web-based firmware upgrade is available from the System tools page by selecting “Firmware Upgrade.” Firmware upgrade is performed by uploading a “patch” file that is specific to the currently installed firmware version. If the device firmware version has fallen multiple versions behind the desired version, it may be necessary to upload multiple patch files. Once the patch files are uploaded, reset the module to perform the firmware upgrade. You will receive more detailed instructions if it is necessary to upgrade the module firmware.

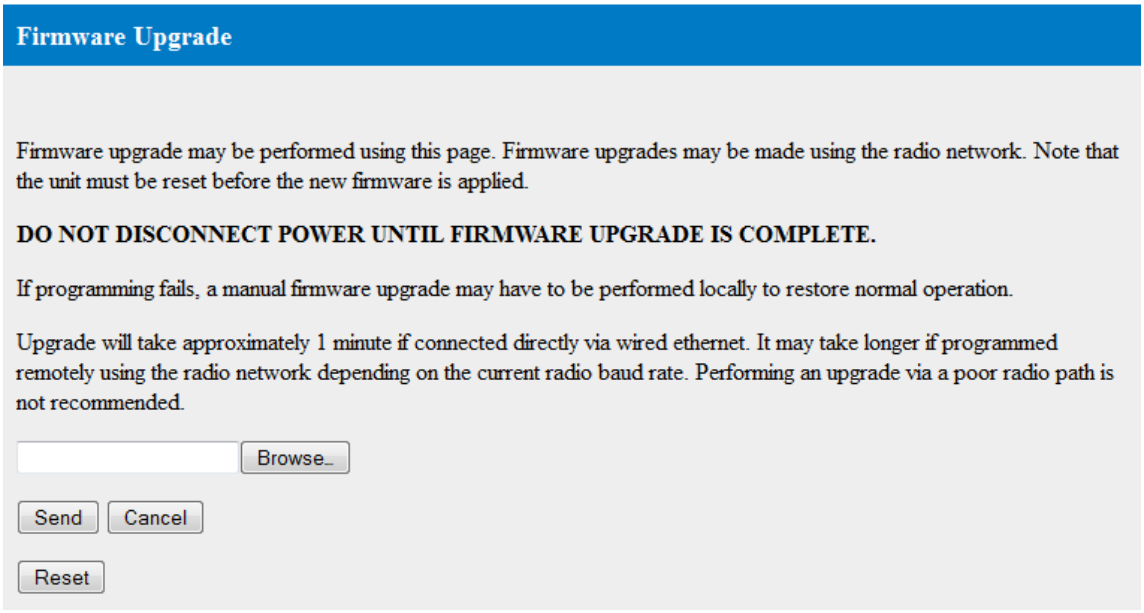


Figure 94 Firmware Upgrades

APPENDIX B - GLOSSARY

Term	Definition
ACK	Acknowledgment.
Access Point	An access point connects wireless network stations (or clients) to other stations within the wireless network and also can serve as the point of interconnection between the wireless network and a wired network. Each access point can serve multiple users within a defined network area. Also known as a base station.
Ad-Hoc Network	Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks. An ad hoc network is any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity.
Antenna Gain	Antennae do not increase the transmission power, but instead focus the signal. Rather than transmitting in every direction (including the sky and ground), antenna focus the signal either more horizontally or in one particular direction. This gain is measured in decibels.
Bandwidth	The maximum data transfer speed available to a user through a network.
Bridge	A bridge connects two local area networks, and is typically used to connect wireless networks to wired networks. Bridges usually transfer messages between networks only when the message destination is on the other network. Messages destined for the network on which they originated are not passed on to the other network. This reduces traffic on the entire network
Collision Avoidance	A network node procedure for pro-actively detecting that it can transmit a signal without risking a collision with transmissions from other network nodes.
Client / Sta / Station	A device on a network that gains access to data, information, and other devices through a server (access point).
Crossover Cable	A cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. The cable is wired so that the signals “crossover,” connecting transmit signal on one side to receiver signals on the other.
CSMA/CA	Carrier sense multiple access/collision avoidance is a “listen before talk” method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states that a collision avoidance method rather than collision detection must be used because the standard employs half-duplex radios, which are capable of transmission or reception, but not both simultaneously. Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.
CSMA/CD	Carrier sense multiple access/collision detection is the access method used on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.
DHCP	Dynamic Host Configuration Protocol is a utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT manager would need to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, an IP address is automatically assigned to it.

Term	Definition
Dial-up	A communication connection via the standard telephone network, or plain old telephone service (POTS).
DNS	Domain name service (DNS) is a program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.
DSL	Digital subscriber line (DSL) is a family of technology protocols for high-speed data, voice and video transmission over ordinary twisted-pair copper POTS (plain old telephone service) telephone wires.
Encryption Key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read. Encryption keys should be kept secret.
Firewall	A device or computer program that keeps unauthorized users out of a private network. Everything entering or leaving a system's internal network passes through the firewall and must meet the system's security standards in order to be transmitted. Often used to keep unauthorized people from using systems connected to the Internet.
Hub	A multiport device used to connect PCs to a network via Ethernet cabling or via 802.11. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multi-Gigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect four computers; a large hub can connect 48 or more.
Hz	Hertz. The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535–1605 kHz, the FM broadcast radio frequency band is 88–108 MHz, and wireless 802.11b/g LANs operate at 2.4 GHz.
IEEE	Institute of Electrical and Electronics Engineers, New York, www.ieee.org. A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.
Infrastructure Mode	An 802.11 setting providing connectivity to an access point. As compared to ad-hoc mode, whereby 802.11 devices communicate directly with each other, clients set in Infrastructure Mode all pass data through a central access point. The access point not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network.
I/O	Input/Output. The term used to describe any operation, program, or device that transfers data to or from a computer.
Internet Appliance	A computer that is intended primarily for Internet access, is simple to set up, and usually does not support installation of third-party software. These computers generally offer customized web browsing, touch-screen navigation, e-mail services, entertainment, and personal information management applications.
IP	Internet Protocol (IP) is a set of rules used to send and receive messages across local networks and the Internet.
IP Telephony	Technology that supports voice, data and video transmission via IP-based LANs, WANs, and the Internet. This includes VoIP (Voice over IP).
IP Address	A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

Term	Definition
IPX-SPX	Internetwork Packet Exchange, is a networking protocol used by the Novell NetWare® operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as Sequenced Packet Exchange (SPX) and NCP, are used for additional error recovery services. SPX is a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications.
ISDN	A type of broadband Internet connection that provides digital service from the customer's premises to the dial-up telephone network. ISDN uses standard POTS copper wiring to deliver voice, data, or video.
ISO Network Model	A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are Physical, Data Link, Network, Transport, Session, Presentation, and Application.
LAN	Local Area Network (LAN) is a system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files, and drives.
Receive Sensitivity	The minimum signal strength required to pick up a signal. Higher bandwidth connections usually have less receive sensitivity than lower bandwidth connections.
Router	A device that forwards data from one WLAN or wired local area network to another.
SNR	Signal to noise ratio (SNR) is the number of decibels difference between the signal strength and background noise.
Transmit Power	The power at which the wireless devices transmits, usually expressed in mW or dBm.
MAC Address	Media Access Control (MAC) address is a unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware, so limiting a wireless network's access to hardware (such as wireless cards) is a security feature employed by closed wireless networks. But an experienced hacker armed with the proper tools can still figure out an authorized MAC address, masquerade as a legitimate address, and access a closed network. Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.
NAT	Network address translation (NAT) is a network capability that enables a number of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.
NIC	Network interface card (NIC) is a type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.
Proxy Server	Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.
RJ-45	Standard connectors used in Ethernet networks. RJ-45 connectors are similar to standard RJ-11 telephone connectors, but RJ-45 connectors can have up to eight wires, whereas telephone connectors have four.

Term	Definition
Server	A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.
Site Survey	The process whereby a wireless network installer inspects a location prior to installing a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.
SSL	Secure Sockets Layer (SSL) is a commonly encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session.
Sub Network or Subnet	Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect together through a router.
Switch	A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.
TCP	Transmission Control Protocol (TCP) is protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a webpage is downloaded from a Web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as single message.
TCP/IP	The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.
VoIP	Voice Over Internet Protocol (VoIP) is a voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).
VPN	Virtual private network (VPN) is a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.
WAN	Wide area network (WAN) is a communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (WLANs).
WEP	Wired Equivalent Privacy (WEP) is a basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.

Term	Definition
Wi-Fi	Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard.

APPENDIX C - POWER CONVERSION

Power Conversion

The following table provides dBm to mW conversion.

Watts	dBm
10 mW	10 dB
13 mW	11 dB
16 mW	12 dB
20 mW	13 dB
25 mW	14 dB
32 mW	15 dB
40 mW	16 dB
50 mW	17 dB
63 mW	18 dB
79 mW	19 dB
100 mW	20 dB
126 mW	21 dB
158 mW	22 dB
200 mW	23 dB
316 mW	25 dB
398 mW	26 dB
500 mW	27 dB
630 mW	28 dB
800 mW	29 dB
1.0 W	30 dB
1.3 W	31 dB
1.6 W	32 dB
2.0 W	33 dB
2.5 W	34 dB
3.2 W	35 dB
4.0 W	36 dB

APPENDIX D - IPERF THROUGHPUT TEST - EXT

This appendix shows how to set up and use the Iperf application to test the throughput of Ethernet modems. Iperf is a tool used to measure the throughput and quality of a network link. Another application, called Jperf ,can also be used, which gives a graphical interface for all results. The following instructions cover Iperf and Jperf, but not the setup and configuration of the modems. Modem setup instructions are provided in earlier sections of this manual.

Materials

- 2 x Ethernet modems configured as a bridge.
- 2 x PC computers with Ethernet ports.
- Suitable power supplies for the Ethernet modems.
- Straight-through Ethernet cables.
- Iperf / Jperf application.

Installation

1. Download the application from the link, http://sourceforge.net/projects/iperf/, and save to a location on your PC.
2. Extract the zip file to the ROOT directory (C:\ ) on your PC.

   The extracted folder contains the main Iperf application as well as the Jperf graphical interface.
3. Copy the extracted folder to the second PC, or download to the second PC and extract as described in steps 1 and 2.

Iperf Application

The Iperf or Jperf application needs to be run on the PC or laptop at each end of the wireless link that is to be tested.

1. At the server PC, open a command prompt by opening the Windows **Start** menu, choosing **Run**, and entering “CMD”.
2. When the Command Prompt screen appears, set the directory to where the Iperf application resides (where it was saved above) and from here run the Iperf server command “iperf –s”. See Figure 95.

   Iperf server application is now running and waiting for a client connection.

   NOTE If you get a security pop up on the PC, select Unblock for the application to run.

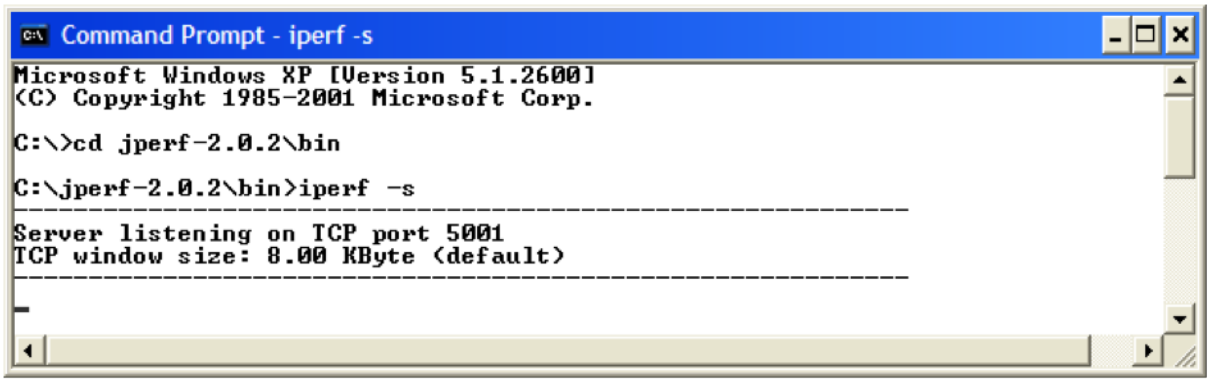


Figure 95 iperf –s Command

3. On the client PC, open up a command prompt and change the directory to jperf-2.0.2\bin as you did for the server. This time enter the iperf command to start the client communication to the server:

   "iperf –c <IP address of Server PC> -w 65535"

   See Figure 96.

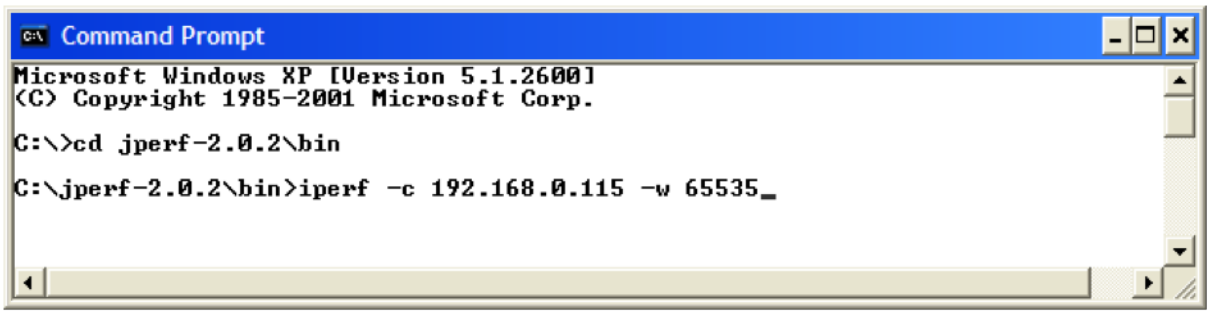


Figure 96 iperf –c Command

This will run a test over the Wi-Fi Link to the server PC and report back results as seen in Figure 97. These results show the bandwidth (throughput) of the test as 16.2 Mbits/sec.

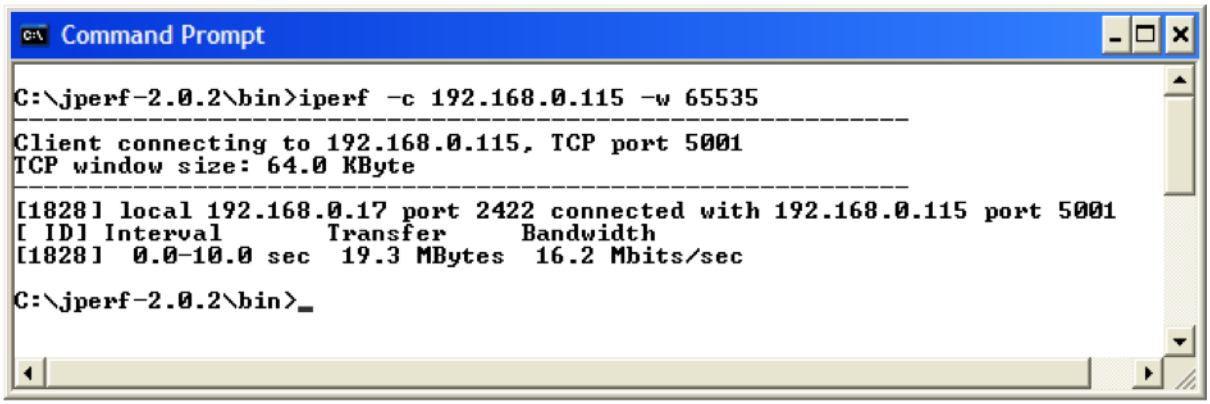


Figure 97 Bandwidth

4. Using the theoretical throughput calculations shown in the following table, you can compare the results with the measured to give an indication of the difference between expected and measured. Keep in mind that the theoretical calculations are best-case possible results.

	240U-E	245U-E-G	245U-E-A	945U-E (20Mhz)	905U-E	805U-E
54 Mbps		27 Mbps	27 Mbps	27 Mbps		
11 Mbps	5 Mbps	5 Mbps	5 Mbps	5 Mbps		
1 Mbps	500 Kbp	500 Kbps	500 Kbps	500 Kbps		
200 Kbps					80 Kbps	
100 Kbps					40 Kbps	
78 Kbps						37 Kbps
19.2 Kbps					7.8 Kbps	6.9 Kbps

In the command line for the client mapping you established the server IP address followed by the –w 65535, -w is the window size and the maximum TCPIP window size is 65535 bytes.

Another entry that can be added is –t <seconds> to run the test for a specific time period.

JPerf Application

Jperf is a graphical interface that runs over the top of Iperf. It will display a graph result from the Iperf test.

To run Jperf:

1. Open a command prompt and change to the jperf-2.0.2: directory and run the “Jperf” application as shown in Figure 98. The Command Prompt screen will disappear and the Jperf Screen will appear as shown in Figure 99.

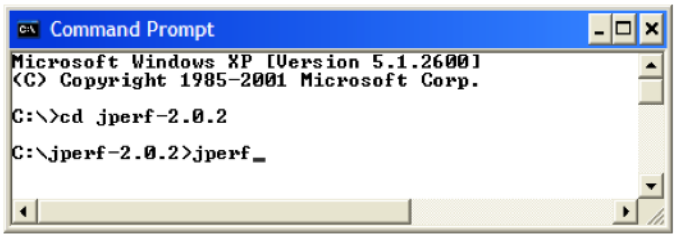


Figure 98 Jperf

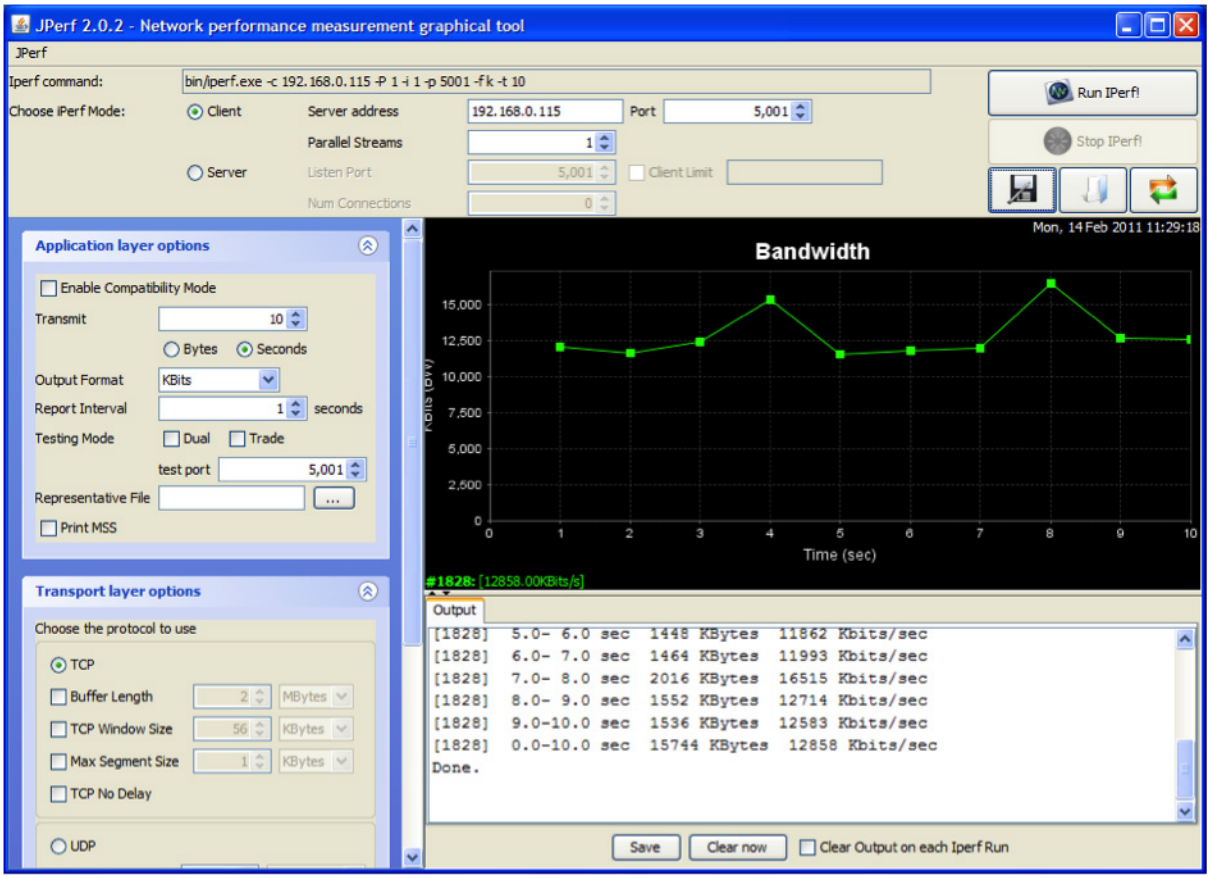


Figure 99 Jperf Screen

2. When the Jperf screen appears, select the Client option for Iperf Mode, and enter the IP address of the server PC. Leave Port as default and click **Run Iperf**.

   The test will run again and the bandwidth (throughput) display will show results of the test.

NOTE Jperf runs using Java technology. Depending on your PC setup, further installation of Java software may be required.

APPENDIX E - GNU FREE DOC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms and Conditions

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification.") Each licensee is addressed as "you."

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and

disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

      These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

      Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

      In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for non-commercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

      The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software

Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Notes:

Eaton's wireless business
www.eaton.com/wireless

North America & Latin America
5735 W. Las Positas Suite 100
Pleasanton, CA 94588
United States
Telephone: +1 925 924 8500

Australia, New Zealand
9/12 Billabong Street
Stafford Queensland 4053
Australia
Telephone: +61 7 3352 8600

China
955 Shengli Road
East Area of Zhangjiang High-Tech Park
Shanghai, 201201
China
Telephone: +86 21 2899 3600

Southeast Asia
2 Serangoon North Avenue 5
06-01 Fu Yu Building, 554911
Singapore
Telephone: +65 6645 9888

Europe
Hein-Moeller-Straße 7-11
53115 Bonn, Germany
Telephone: +49 228 602 5573

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

© 2014 Eaton
All Rights Reserved
Printed in USA
November 2014

Eaton is a registered trademark.

All other trademarks are property
of their respective owners.

Powering Business Worldwide